Cybersécurité - cybercriminalité

Forget, Catherine

Published in:
Les obligations légales de cybersécurité et de notifications d'incidents

Publication date:
2019

Document Version
le PDF de l'éditeur

CYBERSÉCURITÉ – CYBERCRIMINALITÉ : DE L'ENQUÊTE ADMINISTRATIVE À L'ENQUÊTE PÉNALE

Catherine Forget[1353]

A. Introduction

La cybercriminalité est intrinsèquement liée à la cybersécurité. En ce sens, selon la Convention de Budapest, les principales infractions dans un contexte informatique consistent en des atteintes visant la sécurité des systèmes à savoir, « la confidentialité, l'intégrité et la disponibilité des données »[1354]. Cette étroite relation est également évoquée par le Règlement général sur la protection des données[1355] (ci-après « RGPD »). Celui-ci indique que les données doivent être traitées de « façon à garantir une sécurité appropriée » en ce compris « la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle ». De même, la directive « NIS »[1356] rappelle qu'un incident « peut être le résultat d'activités criminelles, à propos desquelles la prévention, les enquêtes et les poursuites sont soutenues par la coordination et la coopération entre les opérateurs de services essentiels, les fournisseurs de service numérique, les autorités compétentes et les services répressifs »[1357].

Il n'en demeure pas moins qu'assurer un haut niveau de sécurité de données et se soucier de respecter scrupuleusement les règles relatives à la protection des données ne permet pas de se soustraire au risque d'être victime d'un acte de cybercriminalité et encore moins, de connaître une faille de sécurité. De nombreux acteurs sont donc susceptibles d'être confrontées à l'obligation de notifier un incident de sécurité à l'Autorité de Protection des

1353. Chercheuse à l'UNamur (NADI) et avocate au Barreau de Bruxelles (JusCogens).

1354. « Rapport explicatif de la Convention sur la cybercriminalité », Conseil de l'Europe, Budapest, 23 novembre 2001, § 35.

1355. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), *J.O.U.E.*, L 119, 4 mai 2016, p. 1 (ci-après « RGPD »). Pour un commentaire général de ce règlement, voy. (e.a.) : K. ROSIER et C. DE TERWANGNE (sous la dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018.

1356. Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.U.E., L 194, 19 juillet 2016, pp. 1–30, (ci-après « directive NIS »).*

1357. Directive NIS, consid. 62.

données (ci-après « APD ») ou le Centre pour la Cybersécurité Belgique (CSIRT national), le Centre de crise, l'autorité sectorielle, le CSIRT sectoriel ou le service d'inspection (ci-après, les autorités NIS), mais aussi, en cas d'infraction pénale, aux autorités policières. Chacune de ces autorités dispose d'un service d'inspection visant à s'assurer du respect des lois soumises à leur contrôle et dont l'issue de la procédure peut aboutir à des sanctions administratives ou pénales.

Dans le cadre de cette contribution, nous tâcherons de mettre en perspective le rôle et les missions dévolues aux services d'inspection de l'APD et des autorités NIS dans le cadre de leurs compétences respectives. Nous verrons qu'ils disposent de diverses techniques d'enquête pouvant s'avérer assez intrusives pour les personnes concernées. Il s'agira également de ne pas perdre de vue qu'à l'inverse des inspecteurs de l'APD, les membres des autorités NIS peuvent avoir la qualité d'officiers de police judiciaire et sont donc tenus de dénoncer les infractions dont ils auraient connaissance auprès du procureur du Roi. En outre, en plus des compétences que leur accorde la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après la loi NIS)[1358], ils peuvent, sous certaines réserves, exercer celles prescrites par le Code d'instruction criminelle (ci-après « CICr ») tel que nous le détaillerons *infra*. Enfin, nous terminerons notre propos en précisant les règles relatives à la protection des données traitées par le service d'inspection de l'APD, des autorités NIS, mais aussi des services de police ainsi que les dispositions pertinentes en cas de flux de données entre ces différentes autorités.

B. Les acteurs

Tant l'APD que l'autorité sectorielle (NIS) disposent d'un service d'enquête visant à s'assurer du respect des dispositions soumises à leur contrôle. À la différence des inspecteurs de l'APD, les inspecteurs du CSIRT peuvent disposer de la qualité d'officiers de police judiciaire ; ce qui n'est pas sans incidence en pratique. Examinons dès lors le rôle et les missions dévolues à chacun de ces services dans le cadre d'une enquête administrative mais également ceux dont sont chargés les officiers de police judiciaire dans le cadre de l'enquête pénale.

1. Le service d'inspection de l'APD

L'APD est responsable du contrôle du respect des principes fondamentaux de la protection des données à caractère personnel, et ce dans le cadre de la loi du 30 juillet 2018[1359]

1358. Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019 (ci-après « loi NIS »).
1359. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel[1360]. À cette fin, elle dispose d'un service d'inspection chargé d'enquêter sur les violations des dispositions relatives à la protection des données[1361]. L'enquête menée par l'APD est ouverte sur initiative du service d'inspection ou du comité de direction en présence d'indices sérieux de l'existence d'une pratique susceptible de porter atteinte aux principes fondamentaux de la protection des données à caractère personnel[1362]. Elle peut également être initiée suite au dépôt d'une plainte ou sur demande de la chambre contentieuse[1363]. Elle est secrète sauf exception légale, et ce, jusqu'au moment du dépôt du rapport de l'inspecteur général auprès de la chambre contentieuse[1364].

L'inspecteur général et les différents inspecteurs de l'APD sont assermentés[1365], mais ils ne disposent pas nécessairement de la qualité d'officier de police judiciaire[1366]. La distinction est importante puisque, sous son ancienne mouture, le projet de loi leur octroyait la qualité « d'officier de police judiciaire auxiliaire du procureur du Roi »[1367] impliquant dès lors une obligation de dénoncer au procureur du Roi les infractions dont ils auraient connaissance[1368]. Or, cette disposition, prévue à peine de sanctions pénales, aurait pu avoir pour conséquence de freiner la dénonciation de certains incidents de sécurité et empêcher l'APD « d'élaborer une politique propre de surveillance de l'application des dispositions légales »[1369], les victimes pouvant craindre que les informations révélées ne constituent des infractions pénales et soient transmises au procureur du Roi[1370]. Il n'en demeure pas moins que les inspecteurs de l'APD restent libres de transmettre volontairement aux autorités judiciaires les infractions dont ils auraient connaissance[1371]. Ils ne sont pas soumis aux directives du procureur du Roi[1372] et conservent une certaine indépendance[1373]. En revanche, ils ne disposent pas d'une compétence générale relative à la

1360. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 25 mai 2018 (ci-après « loi sur l'ADP »), art. 4, § 1er.
1361. Loi sur l'APD, art. 28.
1362. *Ibid.*, art. 63, 1° et 6°.
1363. *Ibid.*, art. 63, 2°.
1364. *Ibid.*, art. 64, § 3.
1365. Ils sont tenus de prêter le serment suivant dans les mains de l'inspecteur général : « Je jure fidélité au Roi, obéissance à la Constitution et aux lois du peuple belge » (Loi sur l'APD, art. 30, § 1er).
1366. Loi sur l'APD, art. 29.
1367. Projet de loi portant création de l'Autorité de protection des données, *Doc. Parl.*, 54- 2648/001, ch. repr., 2016-2017, art. 29, § 1er, p. 64.
1368. Code d'instruction criminelle (ci-après « CICr »), art. 29.
1369. *Ibid.*
1370. APD, « Avis d'initiative relatif au projet de loi réformant la Commission de la protection de la vie privée », *Avis n°21/2017*, p. 22, disponible à l'adresse suivante :
https ://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_21_2017_0.pdf.
1371. Loi sur l'APD, art. 6.
1372. Pour rappel, les officiers de police judiciaire sont nécessairement placés sous la direction et l'autorité du procureur du Roi compétent. (CICr, art. 28*bis*, § 1er).
1373. L'article 52 (5) du RGPD exige en effet qu'ils soient « placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernée ».

recherche des crimes, des délits et des contraventions et ne peuvent exercer les compétences fixées par le Code d'instruction criminelle.

2. Les services d'inspection sectoriel (NIS)

La loi NIS et l'arrêté royal NIS désignent différents services d'inspection compétentes par secteur ou par sous-secteur (ci-après « service d'inspection sectoriel ») et chargé du contrôle du respect des dispositions de la loi et de ses actes d'exécution[1374]. Il s'agit du service public fédéral Economie pour le secteur de l'énergie (à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité)[1375], l'Agence fédérale de Contrôle nucléaire (AFCN) pour ce qui concerne les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité[1376], la Banque Nationale de Belgique (BNB) pour le sous-secteur des établissements financiers[1377], l'Autorité des services et marchés financiers (FSMA) pour le sous-secteur des plates-formes de négociation financière[1378], l'Institut belge des services postaux et des télécommunications (IBPT) pour les infrastructures numériques[1379], le service public fédéral Santé publique pour le secteur de la santé[1380], le service public fédéral Mobilité et Transports[1381] et le service public fédéral Economie pour le secteur des fournisseurs de service numérique[1382].

Les membres du service d'inspection sectoriel sont dotés d'une carte de légitimation et prêtent serment auprès du fonctionnaire dirigeant de leur service[1383]. Le service d'inspection sectoriel peut à tout moment, d'initiative ou sur demande motivée du Centre pour la Cybersécurité Belgique ou encore, sur demande de l'autorité sectorielle, réaliser des contrôles du respect par l'opérateur de services essentiels ou par le fournisseur de service numérique des

1374. Art. 7, § 5 de la loi NIS.
1375. Art. 3, § 4 de l'AR NIS et l'annexe II de l'AR.
1376. Art. 86 de la loi NIS qui insère un article 15 *ter* dans la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.
1377. Art. 95 de la loi NIS qui insère un article 36/47 à la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique.
1378. Art. 90 de la loi NIS qui modifie l'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. Cette disposition précise d'ailleurs que la FSMA peut charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire.
1379. Art. 88 de la loi NIS qui modifie l'article 14, § 1er, 3° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges : l'IBPT est chargé du contrôle du respect des normes suivantes et de leurs arrêtés d'exécution : h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques.
1380. Art. 3, § 4 de l'AR NIS et annexe II de l'AR.
1381. La désignation officielle doit encore intervenir par le Roi.
1382. Ibidem.
1383. Art. 44, § 1, de la loi NIS.

mesures de sécurité et des règles de notification des incidents[1384]. Après chaque inspection, les inspecteurs rédigent un rapport et transmettent copie à l'opérateur de services essentiels ou au fournisseur de service numérique inspecté et à l'autorité sectorielle compétente[1385].

Il est important de souligner qu'à la différence des inspecteurs du service d'inspection de l'APD, les membres du service d'inspection sectoriel peuvent disposer de la qualité d'officiers de police judiciaire[1386]. Ils disposent alors d'une compétence générale relative à la recherche des crimes, des délits et des contraventions et ils agissent sous l'autorité du procureur du Roi[1387]. Du reste, ils sont, à l'instar de tout fonctionnaire, tenus de dénoncer les infractions dont ils auraient connaissance à l'occasion de l'exercice de leur fonction[1388]. En conséquence, lorsqu'ils détectent une activité suspecte à l'occasion de la gestion d'un incident de sécurité par exemple, ils doivent transmettre ces informations au procureur du Roi sous peine de sanctions pénales. Cette exigence pourrait naturellement empêcher certains opérateurs de services essentiels ou fournisseurs de service numérique de porter à la connaissance des autorités NIS un incident de sécurité, les informations transmises étant susceptibles d'entraîner l'ouverture d'une enquête pénale.

Au niveau de l'Union européenne, on indiquera que l'ENISA, l'Agence européenne chargée de la sécurité des réseaux et de l'information, se donne pour mission d'assurer les échanges d'informations et la coopération entre les différents CSIRT nationaux mais aussi, entre les autorités compétentes et les services répressifs de différents États membres[1389]. Elle ne dispose pas de pouvoir d'enquête et n'est dès lors pas dotée d'un service d'inspection qui lui est propre[1390].

3. Les services de police dans le cadre de l'enquête pénale

Les services de police peuvent agir à des fins judiciaires dans le cadre d'une enquête pénale mais aussi à des fins administratives dans le cadre du maintien de l'ordre public[1391]. La police judiciaire, qui fera l'objet de notre propos, exerce ses missions en vue de rechercher les crimes, les délits et les contraventions mais aussi en vue de rassembler les preuves et de livrer les auteurs aux tribunaux chargés de les punir[1392]. Certains services de police sont

1384. Art. 42, § 1, de la loi NIS.
1385. Art. 45, § 1, de la loi NIS.
1386. Art. 44, § 3, de la loi NIS.
1387. Art. 9 CICr.
1388. Art. 29 CICr.
1389. Directive NIS, consid. 62 et art. 12, § 2.
1390. À propos des compétences de l'ENISA, lire la contribution de M. KNOCKAERT dans le présent ouvrage : « La sécurité dans le marché unique numérique européen : le Règlement 2019/881 (« Cybersecurity Act ») » (Chap. 3).
1391. Dans le cadre de leurs missions administratives, ils s'attachent essentiellement au maintien de l'ordre public lequel consiste en la tranquillité, la sécurité et la santé publique et agissent sous la responsabilité du bourgmestre. (Loi du 5 août 1992 sur la fonction de police, art. 14). L'ordre public consiste en la trilogie classique, comprenant la tranquillité, la sécurité et la santé publique. (Nouvelle loi communale du 24 juin 1988, *M.B.*, 13 septembre 1988, art. 133).
1392. CICr, art. 8 ; Loi sur la fonction de police, art. 15.

spécialisés dans l'analyse de systèmes informatiques. Ceux-ci sont organisés à deux niveaux : au niveau national est instituée la *Federal Computer Crime Unit* (FCCU) et au niveau régional, sont mises en place les différentes *Computer Crime Unit* (RCCU) agissant sous la direction des directeurs judiciaires au sein de chaque arrondissement[1393]. Ces deux services collaborent et coexistent afin d'assurer une lutte efficace contre la criminalité informatique.

Au sein de la police judiciaire, tout officier de police judiciaire, qu'il soit ou non « auxiliaire du procureur du Roi »[1394], agit sous la direction du procureur du Roi[1395]. Pour des infractions de moindre importance[1396], la loi indique que les officiers de police judiciaire peuvent exécuter des actes de recherche d'initiative sous réserve d'en informer le procureur du Roi dans un certain délai et selon certaines modalités fixées par directives[1397]. Cette obligation, ni substantielle ni prescrite à peine de nullité[1398], vise à conforter l'autorité et la responsabilité du procureur du Roi quant à la conduite de l'information qu'il dirige et, partant, à assurer l'efficacité de celle-ci[1399]. Enfin, à l'instar de tout fonctionnaire, ils sont tenus de dénoncer les infractions dont ils auraient connaissance à l'occasion de l'exercice de leurs fonctions sous peine de sanctions pénales[1400].

La phase préliminaire de la procédure pénale est dite « inquisitoire » c'est-à-dire secrète, non contradictoire et écrite[1401] afin d'une part, d'assurer l'efficacité de l'enquête[1402] et, d'autre part, de préserver la présomption d'innocence[1403]. Elle se subdivise en deux phases, à savoir, l'information menée par le procureur du Roi[1404] et l'instruction dont la direction est assurée par le juge d'instruction[1405]. L'information a pour objet la recherche des infractions, leurs auteurs et les preuves[1406]. Elle s'exécute de manière réactive ou

1393. A ce propos, voy. Comité P, « La police intégrée et la recherche forensique dans un environnement informatisé », 2018, disponible à l'adresse suivante : https ://comitep.be/document/onderzoeksrapporten/2018-06-21%20Enquete%20forensique.pdf.
1394. Loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, *M.B.*, 5 janvier 1999, art. 138 et 138*bis*.
1395. Loi sur la fonction de police, art. 8.
1396. A. JACOBS, A. SADZOT, V. GUERRA, A. HOLLANDERS et G. FALQUE, *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, 2018, I 42 / 01 – I 42 /67, p. 14.
1397. CICr, art. 28*ter*, § 2, al. 1er.
1398. Cass., 20 octobre 2015, P.15.0789.N, *Pas.*, 2015/10, pp. 2379-2383.
1399. *Ibid.*
1400. CICr, art. 29.
1401. Historiquement, deux systèmes s'opposaient. Le système accusatoire suppose que la procédure démarre par le biais d'un accusateur, souvent la victime, le juge ayant souvent le rôle d'arbitre. La procédure inquisitoire implique par contre une enquête préliminaire. Elle est secrète, écrite et unilatérale. Notre système est une conciliation des deux approches : la phase préliminaire du procès pénal est dite inquisitoire alors que la phase de jugement est en grande partie accusatoire. (M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 22-28)
1402. *Doc. parl.*, Chambre, 1996-1997, n°857/1, p. 7.
1403. Selon l'article 6, § 2 de la Convention européenne des droits de l'Homme : « Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie ».
1404. CICr, art. 28*bis*.
1405. *Ibid.*, art. 55.
1406. *Ibid.*, art. 28*bis*.

proactive[1407]. L'instruction, par contre, consiste en la recherche des auteurs et des preuves relativement à des faits commis et connus[1408]. En principe et sous réserve de la mini-instruction[1409], seul le juge d'instruction est habilité à poser un acte de contrainte susceptible de porter atteinte aux droits et libertés individuelles[1410]. En effet, celui-ci instruit à charge et à décharge de manière « indépendante et impartiale » alors que le procureur du Roi assume « le rôle de la partie poursuivante »[1411] et « ne peut donc être considéré comme impartial »[1412]. Cette répartition des rôles semble toutefois s'assouplir au fil du temps compte tenu de la multiplication des exceptions permettant au procureur du Roi d'agir dans des matières réservées au juge d'instruction,[1413] et ce, à l'heure où la place et le rôle du magistrat instructeur font l'objet de vives discussions[1414].

1407. Selon l'article 28*bis*, § 2 du CICr, l'information s'étend à l'enquête proactive. Celle-ci consiste en la recherche, la collecte, l'enregistrement et le traitement de données et d'informations, sur la base d'une *suspicion raisonnable* que des faits punissables soit, vont être commis soit, ont été commis mais ne sont pas encore connus. Par opposition à l'enquête réactive, elle se caractérise par une certaine proactivité puisque l'acte répréhensible n'est pas encore connu des enquêteurs sans pour autant être insoupçonné. (M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, Bruxelles, Éditions Larcier, 2012, p. 266.)
1408. CICr, art. 55. Notons que L. KENNES nuance en écrivant que : « Par arrêt du 4 février 1997, la Cour de cassation a précisé que la mise à l'instruction est justifiée non seulement pour un fait dans une certaine mesure établi mais aussi pour un fait ne faisant pas l'objet d'un indice ou d'une suspicion concernant l'existence d'une infraction. Dans ce dernier cas, il relève de la mission du juge d'instruction de récolter les preuves de l'existence de cette infraction. (…) Par conséquent, le juge d'instruction est compétent dès qu'un fait susceptible de révéler la commission d'une infraction est connu ». (L. KENNES, *Manuel de la preuve en matière pénale*, Malines, Kluwer, 2009, p. 29.)
1409. La mini-instruction, réglementée par l'article 28 *septies* du CICr, permet au procureur du Roi de requérir du juge d'instruction l'accomplissement d'un acte d'instruction sans pour autant réellement ouvrir une instruction. Certains actes restent néanmoins de la compétence unique du juge d'instruction notamment l'interception des communications et l'observation avec des moyens techniques dans un domicile visés respectivement par les articles 90*ter* et 89*ter* du CICr en raison de l'ingérence particulièrement importante pour les droits et libertés des personnes concernées.
1410. CICr, art. 28, § 3.
1411. *Ibid.*, art. 28*bis*.
1412. C. Const., 25 janvier 2017, arrêt n°6/2017, C 6325 et 6326, B. 5.2.
1413. Depuis l'adoption de la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, (*M.B.*, 12 mai 2003) le procureur du Roi peut procéder à des méthodes particulières de recherche telles l'observation, l'infiltration et le recours aux indicateurs, méthodes considérées comme particulièrement invasives pour les droits et libertés fondamentales. La loi du 25 décembre 2016 s'inscrit dans cette même dynamique, celle-ci offrant des nouvelles méthodes aux enquêteurs ou clarifiant le cadre légal préexistant tout en laissant transparaître un accroissement des compétences du procureur du Roi (Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017). Pour un commentaire de la loi du 25 décembre 2016 : voy. C. CONINGS et S. ROYER, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N.C.*, 2017/4, pp. 313-320 ; V. FRANSSEN et S. TOSZA, « Vers plus de droits pour le justiciable sur Internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information » in *Les droits des justiciables face à la justice pénale*, Limal, Anthemis, 2017, pp. 205 – 249).
1414. A ce propos, voy. M.-A. BEERNAERT, « Du juge d'instruction au juge de l'enquête : raisons et contours de la réforme proposée », *in La figure du juge d'instruction : réformer ou supprimer ?*, Larcier, 2017, pp. 21-28 ; L. KENNES et D. SCALIA, *Du juge d'instruction vers le juge de l'enquête : analyse critique et de droit comparé*, Bruxelles, Anthemis, 2017.

Au niveau européen, le Centre européen de lutte contre la cybercriminalité au sein d'Europol (EC3) s'est donné pour mission de contribuer à la lutte contre la cybercriminalité. À cette fin, le Centre sert d'appui aux opérations des services répressifs, constitue un point névralgique d'échange d'informations sur les activités criminelles et offre une expertise en matière de cybercriminalité. À titre illustratif, récemment, le Centre a participé à des opérations de grande envergure, réalisées de manière coordonnée et fondées sur des renseignements contre les principales menaces en matière de cybercriminalité au moyen d'enquêtes et d'opérations transfrontières[1415]. Il a également porté le projet *NoMoreRansom*[1416] associant des agences répressives et des acteurs privés afin d'aider les victimes de logiciels malveillants chiffrant leurs données dans le but d'obtenir une somme d'argent (les « rançongiciels »). Le centre ne dispose pas d'un service d'enquête qui lui est propre mais il peut prêter son concours à toutes les activités et à tous les échanges d'informations ayant lieu avec tout membre d'une équipe commune d'enquête dans les limites du droit des États membres dans lesquels cette équipe opère[1417]. En ce sens, le EC3 coopère également avec des organismes européens tels que l'ENISA. En effet, suite à un accord signé en 2014, l'ENISA fait partie du comité du programme du centre EC3[1418] au même titre que le centre EC3 fait, à son tour, partie du groupe permanent de l'ENISA[1419]. Cette coopération vise notamment à permettre : les échanges d'expertise et de connaissances spécialisées, la production de rapports de situation d'ordre général, des rapports découlant d'analyses stratégiques et de bonnes pratiques, le renforcement des capacités de ces institutions, grâce à des formations et des campagnes de sensibilisation et ce, afin d'assurer la sécurité des réseaux et de l'information au niveau européen.

C. Les compétences

Dans le cadre d'une enquête administrative, le service d'inspection de l'APD et le service d'inspection sectoriel (NIS) disposent d'un large panel de compétences. Les inspecteurs peuvent par exemple, procéder à l'audition de personnes, pénétrer dans une entreprise, consulter des systèmes informatiques et copier les données qu'ils contiennent. Au besoin, dans l'exercice de leurs missions, ils peuvent également requérir l'assistance des services de police lesquels peuvent également exécuter des actes de recherche lorsqu'ils agissent sous l'autorité du procureur du Roi ou du juge d'instruction.

1415. A ce propos, voy. Le rapport d'Europol : « Internet Organised Crime Threat Assessment (IOCTA) 2018 » disponible sur https ://www.europol.europa.eu/Internet-organised-crime-threat-assessment-2018.
1416. A ce propos voy. le site Internet : https ://www.nomoreransom.org/.
1417. Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, art. 5.
1418. Ce groupe conseille le directeur de l'Agence quant au programme de travail annuel et quant à ses priorités.
1419. Accord de coopération stratégique du 26 juin 2014 signé entre ENISA et Europol, disponible à l'adresse suivante : https ://www.enisa.europa.eu/news/enisa-news/prs-in-french/lutte-contre-la-cybercriminalite-signature-d2019un-accord-de-cooperation-strategique-entre-l2019enisa-et-europol/at_download/file.

1. Le service d'inspection de l'APD

Pour instruire un dossier, l'inspecteur général et les inspecteurs disposent de compétences importantes puisqu'ils peuvent :
- procéder à l'identification de personnes ou à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé[1420] ;
- auditionner des personnes[1421] lesquelles peuvent être assistées d'un conseil[1422] ;
- mener une enquête écrite[1423].

En outre, lorsqu'ils ont des raisons de penser qu'une infraction aux principes fondamentaux de la protection des données à caractère personnel ou relative aux lois dont ils assurent le contrôle est commise, ils peuvent :
- pénétrer à tout moment dans l'entreprise, le service, ou tout autre endroit pour procéder à un examen sur place afin d'y faire des constatations matérielles[1424] ;
- pénétrer dans des espaces habités moyennant accord de l'occupant ou, à défaut, une autorisation du juge d'instruction[1425] ;
- consulter des systèmes informatiques et copier les données qu'ils contiennent ;
- accéder à des informations par voie électronique ;
- saisir ou mettre sous scellés des biens ou des systèmes informatiques[1426].

Dans l'exécution de leurs missions, l'inspecteur général et les inspecteurs doivent être en possession de la carte de légitimation de leur fonction qu'ils doivent immédiatement produire sur demande[1427].

Par ailleurs, l'inspecteur général et les inspecteurs peuvent ordonner la suspension, la limitation ou le gel temporaire du traitement de données qui font l'objet d'une enquête s'il convient d'éviter une situation susceptible de causer un préjudice grave, immédiat et difficilement réparable[1428]. En ce cas, les parties concernées peuvent être entendues par l'inspecteur général ou un inspecteur pour faire valoir leurs griefs dans un délai de cinq jours à partir de l'exécution de la mesure[1429]. Le service d'inspection doit prendre une décision motivée fixant la durée de la mesure provisoire qui peut être de trois mois, prorogeable d'une nouvelle durée de trois mois au maximum[1430]. Les parties concernées disposent

1420. Loi sur l'APD, art. 73.
1421. *Ibid.*, art. 74.
1422. *Ibid.*, art. 75, § 1er.
1423. *Ibid.*, art. 76.
1424. *Ibid.*, art. 78.
1425. *Ibid.*, art. 79, § 1er.
1426. *Ibid.*, art. 44.
1427. *Ibid.*, art. 31.
1428. *Ibid.*, art. 70, al. 1er.
1429. *Ibid.*, art. 70, al. 2.
1430. *Ibid.*, art. 70, al. 3.

d'un droit de recours à l'encontre de cette décision devant la chambre contentieuse, ce recours étant non-suspensif[1431].

Il est important de préciser que l'article 66, § 2 de la loi sur l'APD prévoit une obligation de collaboration dans le chef des personnes qui font l'objet d'un contrôle[1432]. Le non-respect de cette obligation n'est cependant pas prévu à peine de sanctions pénales ou administratives. On notera également que l'inspecteur général et les inspecteurs peuvent, par demande motivée, requérir l'assistance de la police dans l'exercice de leurs missions[1433].

2. Le service d'inspection sectoriel (NIS)

Tant dans le cadre de démarches administratives, que dans le cadre de la constatation d'infractions par procès-verbal, le service d'inspection sectoriel peut :

- pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'opérateur de services essentiels mais aussi les locaux habités sous réserve d'une ordonnance du juge d'instruction[1434] ;
- prendre connaissance sur place et obtenir une copie de la politique de sécurité des systèmes et réseaux d'information, des rapports d'audits, de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission[1435] ;
- procéder à tout examen, contrôle et audition[1436] ;
- requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission[1437] ;
- prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'opérateur de services essentiels et dont ils estiment l'audition nécessaire pour l'exercice de leur mission[1438] ;
- solliciter des informations auprès de certains membres du personnel visés tant par la loi relative à l'Agence fédérale du contrôle nucléaire mais aussi par la loi relative à la sécurité et la protection des infrastructures critiques[1439] ;
- consulter tous les supports d'information/systèmes informatiques et les données qu'ils contiennent dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme

1431. *Ibid.*, art. 71, al. 1er.
1432. *Ibid.*, art. 66, § 2.
1433. *Ibid.*, art. 65.
1434. Loi NIS, art. 44, § 3, 1°.
1435. *Ibid.*, art. 44, § 3, 2°.
1436. *Ibid.*, art. 44, § 3, 1°.
1437. *Ibid.*, art. 44, § 3, 3°.
1438. *Ibid.*, art. 44, § 3, 4°.
1439. *Ibid.*, art. 44, § 3, 6°. Plus précisément, il s'agit des membres visés par l'article 9 de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, pour les besoins de l'exécution des dispositions de la présente loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques

lisible et intelligible qu'ils ont demandée[1440]. Sur cette base ils peuvent également procéder à l'extension d'une recherche dans un système informatique sous réserve de disposer de l'autorisation d'un juge d'instruction[1441].

Afin de faciliter la mise en œuvre de leurs missions, le service d'inspection sectoriel peut requérir l'assistance des services de la police fédérale ou locale[1442].

Il est important de préciser que les compétences précitées leur sont attribuées « sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle »[1443]. Autrement dit, les membres du service d'inspection sectoriel peuvent procéder aux différentes méthodes d'enquête prescrites par le Code d'instruction criminelle sur demande du procureur du Roi ou du juge d'instruction[1444]. Une limite s'impose toutefois dans la mesure où ils ne sont pas officiers de police judiciaire « auxiliaire du procureur du Roi », la loi leur attribuant des mesures spécifiques. À titre illustratif, en cas de flagrant délit, seuls ces derniers peuvent exercer les compétences attribuées au procureur du Roi[1445] telle que la perquisition en vue de constater la commission d'une infraction[1446]. Nous y reviendrons dans la section suivante. Enfin, à la différence de la loi APD, la loi NIS ne prévoit aucune obligation de collaboration à l'égard des personnes faisant l'objet d'un contrôle.

3. Les officiers de police judiciaire

Les compétences des officiers de police judiciaire, en ce inclus les membres du service d'inspection du CSIRT, diffèrent selon qu'ils agissent sur demande du procureur du Roi, au stade l'information, ou sur demande du juge d'instruction, au stade de l'instruction. L'arsenal étant important, nous nous limiterons dans le cadre de cette contribution, aux actes d'enquête susceptibles d'être requis en cas de violation de données à caractère personnel au sens de l'article 4, 12) du RGPD ou en cas d'un incident de sécurité au sens de l'article 6, 13° de la loi NIS[1447]. Ces actes d'enquête s'inspirent de la Convention de Budapest[1448], adoptée au niveau du Conseil de l'Europe et ratifiée par la Belgique en

1440. Loi NIS, art. 44, § 6.
1441. *Ibid.*, art. 44, § 7.
1442. *Ibid.*, art. 44, § 3, 5°.
1443. *Ibid.*, art. 44, § 3, 1°.
1444. CICr, art. 28*ter*, § 3 et 56, § 2.
1445. *Ibid.*, art. 49 et 52. A ce propos, voy. C. De Valkeneer, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 45.
1446. CICr, art. 46.
1447. Pour un approfondissement sur ces actes d'enquête, voy. C. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N.C.*, 2017/4 ; V. Franssen et S. Tosza, « Vers plus de droits pour le justiciable sur Internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information » in *Les droits des justiciables face à la justice pénale*, Limal, Anthemis, 2017, p. 220 et suivantes ; C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique, vers un cadre (plus) strict ? », *R.D.T.I.*, n°66-67, 2017, pp. 25-52.
1448. Convention sur la cybercriminalité, signée à Budapest, le 23 novembre 2001, *S.T.C.E.*, n°185.

2012[1449]. Cette Convention offre aux États parties un cadre contraignant en matière de procédure pénale dans le domaine de la cybercriminalité[1450]. Avant d'examiner les différents actes d'enquête, rappelons certains principes généraux relatifs à la collecte de preuves en matière pénale.

a) Principes généraux : la liberté de la preuve et les limites

En vertu du principe de la liberté de l'administration de la preuve[1451], le procureur du Roi et le juge d'instruction sont libres du choix des moyens qu'ils utilisent pour rassembler et produire les informations visant à démontrer la véracité de l'accusation[1452]. Néanmoins, trois limites fondamentales encadrent l'activité probatoire de ces autorités, à savoir le respect des critères de légalité, de régularité et de loyauté des preuves rassemblées et produites[1453]. Partant, ces autorités sont tenues de respecter les dispositions légales relatives à l'acte d'information ou d'instruction posé[1454] mais aussi de respecter les principes généraux du droit[1455]. Elles ne peuvent pas, en principe, commettre d'infractions dans leur mission de récolte de preuves[1456]. Le critère de loyauté implique, selon la doctrine, que la preuve soit obtenue dans le respect du droit, en travaillant avec franchise, probité et *fair-play*[1457]. Il revient ensuite au juge du fond d'apprécier la valeur probante des éléments sur lesquels il fonde sa conviction et que les parties ont pu librement contredire[1458].

À ce stade, précisons déjà que la violation d'une règle de procédure n'emporte pas nécessairement la nullité de la preuve. En effet, l'article 32 du titre préliminaire du Code pénal énonce : « La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :

1449. Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, faites à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012.
1450. Convention sur la cybercriminalité, *op. cit.*, art. 16 à 21.
1451. On entend par « administration des preuves » la manière de rassembler celles-ci, les procédés employés pour les produire (P. THEVISSEN, « Preuve en droit pénal », in *Postal Mémorialis – Lexique du droit pénal et des lois spéciales*, Kluwer, septembre 2014, p.185/5).
1452. Comme le précise DE VALKENEER : « Le principe de la liberté des preuves est de jurisprudence et de doctrine constantes en droit pénal belge. Il découle d'une interprétation des articles 154 et suivants, 189 et suivants et 290 et suivants CICr. ». (DE VALKENEER, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 71 et suivants).
1453. L. KENNES, *Manuel de la preuve en matière pénale*, Malines, Kluwer, 2009, pp. 24-29.
1454. *Ibid.*, p. 29.
1455. Comme le précise la doctrine, « la notion de régularité de la preuve renvoie aux valeurs considérées comme essentielles à une bonne administration de la justice et qui ne sont pas formulées, en tant que telles, dans un texte. Il s'agit, en d'autres termes, des exigences de dignité de la justice et de loyauté dans la recherche des preuves qui, toutes deux, touchent au respect de la personne, de la dignité humaine, des principes généraux du droit et des droits de la défense. » (F. KUTY, « Le droit de la preuve à l'épreuve des juges », *J.T.*, 2005/20, n° 6182, p. 351.).
1456. J. DE CODT, « Preuve pénale et nullités », *Rev. dr. pén.*, 2009, pp. 648-649.
1457. C. DE VALKENEER, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2018, p. 71 et s.
1458. Cass., 6 septembre 1971, *Pas.*, 1972, I, 12 ; Cass., 24 septembre 2003, RG P.03.1053.F

le respect des conditions formelles concernées est prescrit à peine de nullité, ou ; l'irrégularité commise a entaché la fiabilité de la preuve, ou ; l'usage de la preuve est contraire au droit à un procès équitable. ». Cette disposition, insérée par la loi du 24 octobre 2013[1459], fait suite une longue controverse doctrinale et jurisprudentielle[1460] dont les tournants furent marqués par un premier arrêt de la Cour de cassation en 2003[1461] puis un second en 2005[1462]. On précisera à toutes fins utiles que cette jurisprudence, dite « Antigone », a été validée tant par la Cour européenne des droits de l'Homme[1463] – sous réserve du respect de certains critères[1464] – que par la Cour constitutionnelle[1465] .

L'analyse de cette jurisprudence dépasserait le cadre de cette contribution. Nous pouvons toutefois succinctement relever certains éléments relatifs à chacun des critères précités. Concernant les formes prescrites à peine de nullité, celles-ci sont rares. Il s'agit par exemple des règles relatives à l'emploi des langues[1466] ou encore de certaines règles relatives à la saisie

1459. Loi du 24 octobre 2013 modifiant le titre préliminaire du Code de procédure pénale en ce qui concerne les nullités, *M.B.*, 22 novembre 2013. Pour un premier commentaire de cette loi, voy. J. DE CODT, « La nouvelle loi sur les nullités : un texte inutile ? », *Rev. dr. pén.*, 2014, pp. 258-259.
1460. Depuis la fin des années 1990, la jurisprudence considère qu'une preuve recueillie irrégulièrement ou illégalement n'est pas forcément nulle. En revanche, entre les années 1920 jusqu'au début des années 1990, les juridictions pénales appliquaient strictement le principe d'exclusion de la preuve illicite considérant que « Les preuves sur lesquelles l'action publique est fondée et qui sont soumises à la libre appréciation du juge pénal doivent avoir été obtenues légalement » (Cass., 13 mai 1986, *Pas.*, 1986, I, p. 1107).
1461. En 2003, la Cour de cassation casse un arrêt écartant les résultats d'une mesure de perquisition opérée de manière irrégulière. (Cass., 14 octobre 2003, *R.W.*, 2003-2004, p. 814). Pour des premiers commentaires, voy. F. KUTY, « La règle de l'exclusion de la preuve illégale ou irrégulière : de la précision au bouleversement », obs. sous Cass., 14 octobre 2003, *R.C.J.B.*, 2004, pp. 408-438 ; F. SCHUERMANS, « De nieuwe cassatierechtspraak inzake de sanctionering van het onrechtmatig verkregen bewijs : doorbrak of bres ? », *R.A.B.G.*, 2004, pp. 337-357 ; P. TRAEST, « Onrechtmatig verkregen doch bruikbaar bewijs : het Hof van Cassatie zet de bakens uit », *T. Strafr.*, 2004, pp. 133-143 ; S. BERNEMAN, « Sanctionering van onrechtmatig verkregen bewijsmateriaal : een inleiding tot het Antigoon-arrest van 10 oktober 2003 », *T. Strafr.*, 2004, pp. 2-39.).
1462. En 2005, dans le cadre de l'arrêt Manon, la Cour de cassation ajoute des critères supplémentaires que le juge peut prendre en considération pour apprécier la recevabilité de la preuve à savoir, « notamment, la circonstance que l'illicéité commise est sans commune mesure avec la gravité de l'infraction dont l'acte irrégulier a permis la constatation, ou que cette irrégularité est sans incidence sur le droit ou la liberté protégés par la norme transgressée » (Cass., 2 mars 2005, *J.T.*, n° 6174, 12/2005, p. 212. Voy. également : M.-A. BEERNAERT, « La fin du régime d'exclusion systématique des preuves illicitement recueillies par les organes chargés de l'enquête et des poursuites », *J.L.M.B.*, 25/2005, obs. sous Cass., 2 mars 2005, p. 1094).
1463. Cour eur. D.H., 28 juillet 2009, Davies c. Belgique, *Rev. dr. pén.*, 2010, p. 312 et la note de N. COLETTE-BAZECQZ, « L'admissibilité des preuves irrégulières au regard du droit à un procès équitable : la jurisprudence 'Antigoon' sous la loupe de la Cour européenne des droits de l'homme ».
1464. Cour eur. D.H., 31 janvier 2017, aff. Kalnéniené c. Belgique, *J.L.M.B.*, 2017, p. 447.
1465. C. const., 22 décembre 2010, *J.L.M.B.*, 2011, p. 298 ; *R.A.B.G*, 2011, p. 563 ; et la note de F. SCHUERMANS, « Na Straatsburg betonneert nu ook Grondwettelijk Hof de Antigoon-rechtspraak ».
1466. Loi du 13 juin 1935 concernant l'emploi des langues en matière judiciaire, *M.B.*, 22 juin 1935, art. 40. Voy. B. DEJEMEPPE, « L'emploi des langues dans la justice pénale après la sixième réforme de l'État et quelques autres questions », *in* D. I BOUJOUIOUKLIEV et P. DHAEYER, *La théorie des nullités en droit pénal*, Limal, Anthemis, 2014, pp. 149 et s.

immobilière[1467]. Dans un contexte informatique, les règles relatives à l'interception des communications étaient jusqu'à peu prescrites à peine de nullité entraînant dès lors, automatiquement, l'impossibilité de l'utilisation au cours du procès pénal des écoutes réalisées irrégulièrement[1468]. Suite à l'adoption de la loi pot-pourri II[1469], ces règles ne sont plus prescrites à peine de nullité, ce à quoi la Cour constitutionnelle ne s'est pas opposée[1470], en dépit de la gravité de l'ingérence qu'emporte une telle mesure pour les droits et libertés des personnes concernées[1471]. Concernant les preuves peu fiables, l'article 32 du Titre préliminaire du Code pénal exige, en plus, un lien de causalité entre l'irrégularité commise et le manque de fiabilité de celles-ci[1472], lien qui peut être difficile à démontrer. Enfin, concernant l'atteinte au droit à un procès équitable[1473], la Cour de cassation a récemment considéré qu'il y a lieu de faire application du principe de proportionnalité et, dès lors, de prendre en considération le poids de l'intérêt public à la poursuite de l'infraction et au jugement de son auteur, mis en balance avec l'intérêt de l'individu à ce que les preuves à sa charge soient recueillies régulièrement[1474]. Pour chacun des trois critères, l'exercice d'analyse est donc assez périlleux et a pour conséquence de mener à un renversement de principe dans le cadre du procès pénal ; à savoir une recevabilité des preuves irrégulières sauf exception.

1467. Selon l'article 35*bis*, § 1er CICr : « Lorsque les choses paraissant constituer un avantage patrimonial tiré d'une infraction sont des biens immeubles, la saisie immobilière conservatoire sera faite par exploit d'huissier signifié au propriétaire et contenant, *à peine de nullité*, la copie du réquisitoire du procureur du Roi, ainsi que les différentes mentions visées aux articles 1432 et 1568 du Code judiciaire, et le texte du troisième alinéa du présent article. »

1468. CICr, art. 90*quater*.

1469. Loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, *M.B.*, 19 février 2016.

1470. Celle-ci a considéré que cela « ne diminue pas la protection contre les atteintes à la vie privée des personnes résultant des mesures d'écoutes et d'enregistrements des communications. » (C.C., arrêt n°148/2017 du 21 décembre 2017, B.28).

1471. Le législateur considère en effet que « Ce n'est pas parce que la forme peut être entachée à un moment déterminé que le contenu en perd toute valeur. Ce n'est que si la forme a failli et que de ce fait le contenu est devenu caduc et non fiable que l'acquittement doit suivre. Il appartient à un juge indépendant et impartial de faire cette évaluation ». voy. Projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, Exposé des motifs, *Doc. parl.*, Ch. Repr., sess. Ord. 2015-2016, n°54-1418/001, p. 62.

1472. Ainsi, comme le souligne F. LUGENTZ : « Pour mener à une telle conclusion, il faut en effet, d'abord, que le juge fasse le constat que la preuve a été obtenue de manière irrégulière, en violation des règles au sens large qui l'entourent et, ensuite, que cette irrégularité compromet sa fiabilité (un lien causal entre les deux est ainsi requis » (F. LUGENTZ, *La preuve en matière pénale*, Limal, Anthemis, 2017, p. 66.).

1473. Cette notion a été définie au fil de la jurisprudence belge et européenne et vise notamment, le droit au silence et le droit de ne pas participer à sa propre incrimination, le droit à l'assistance d'un avocat ou la présomption d'innocence. A ce propos voy. le Guide sur l'article 6 de la Convention européenne des droits de l'Homme, Droit à un procès équitable (volet pénal), Conseil de l'Europe, Strasbourg, 2014, disponible sur https ://www.echr.coe.int/Documents/Guide_Art_6_criminal_FRA.pdf.

1474. Cass., 18 janvier 2017, P.16.0626.F, *Rev. dr. pén.*, 2017/6, p. 630-655.

Particulièrement important dans le cadre de la dénonciation d'infraction ou de la coopération volontaire, à la différence des autorités répressives, les tiers tels que les inspecteurs de l'APD, ne sont pas soumis au respect des règles de procédure pénale ou aux exigences de loyauté et de bonne administration de la justice[1475]. Dès lors, selon la Cour de cassation, les preuves recueillies de manière irrégulière par un tiers fortuitement ou non sont en principe admissibles pour autant qu'il n'agisse pas sur demande des autorités[1476] ou dans une intention frauduleuse voire à dessein de nuire[1477]. Il n'en serait *a fortiori* pas de même pour les inspecteurs du CSIRT, compte tenu de leur qualité d'officier de police judiciaire : les règles relatives à la recevabilité des preuves par ceux-ci devront très probablement être examinées plus rigoureusement que pour les informations collectées par les enquêteurs de l'APD.

b) Les actes d'enquête au stade de l'information

Le procureur du Roi dispose d'un « devoir et un droit général d'information »[1478]. Dans ce cadre, il peut, avec l'aide des services de police[1479], notamment procéder à une préservation de données, à l'identification d'un utilisateur de services de communications électroniques, à une recherche dans un système informatique et à une saisie des données et enfin au blocage de site Internet.

i. La préservation de données

En cas d'incident de sécurité, il peut être nécessaire de réagir dans les plus brefs délais dans la mesure où les données informatiques sont particulièrement volatiles et dès lors, susceptibles de perte ou de modifications. Or, dans l'urgence, les services de police ne disposent pas toujours des autorisations nécessaires pour pouvoir pénétrer dans un système informatique et y saisir les données. Dès lors, dans l'attente, ils peuvent ordonner, à une personne physique ou morale, la conservation immédiate des données en sa possession ou sous son

1475. Pour une première étude et les évolutions jurisprudentiels à ce propos voy. O. LEROUX et Y. POULLET, « En marge de l'affaire Gaia : de la recevabilité de la preuve pénale et du respect de la vie privée », *R.G.C.B.*, n° 3, pp. 163-176. Plus récemment, voy. F. LUGENTZ, *La preuve en matière pénale*, Limal, Anthemis, 2017.

1476. Cass., 17 janvier 1990, *Pas.*, I, p. 588.

1477. Cass., 17 novembre 2015, P.150880.N/1. La Cour a considéré ce qui suit : « 3. Ni l'article 8.1 de la Convention, ni l'article 314*bis* du Code pénal n'interdisent le simple enregistrement d'une conversation par un participant à cette conversation à l'insu des autres participants. 4. Celui qui, en vue de l'administration de la preuve dans un litige impliquant les participants à une conversation, fait usage d'un enregistrement effectué par lui de cette conversation à laquelle il a pris part, n'agit pas avec l'intention frauduleuse ou le dessein de nuire visés par l'article 314*bis*, § 2, alinéa 2, du Code pénal. ». Dans le même sens, voy. Cass., 8 janvier 2014, R.G. P.13.1935.F. www.cass.be.

1478. CICr, art. 28, § 1er.

1479. *Ibid.*, art. 28*ter*, § 3.

contrôle,[1480] et ce, pendant une période maximale de nonante jours[1481]. La décision doit être écrite et motivée et indiquer : le nom et qualité de l'officier de police judiciaire qui demande la conservation, l'infraction qui fait l'objet de la recherche, les données qui doivent être conservées et la durée de conservation des données[1482]. En cas d'urgence, la demande de conservation peut être ordonnée verbalement, elle doit toutefois être confirmée par écrit dans les plus brefs délais[1483]. Les personnes conservant les données sont tenues de veiller à leur intégrité et leur sécurité[1484] mais aussi de garder le secret dont le non-respect est sanctionné dans les mêmes conditions que celles visées par l'article 458 du Code pénal ; à savoir le secret professionnel[1485]. Le refus de collaboration et la disparition, destruction ou modification des données conservées sont punissables d'une peine d'emprisonnement de six mois à un an ou d'une peine d'amende[1486] de vingt-six euros à vingt mille euros ou d'une de ces peines seulement[1487].

Si le système informatique visé n'est pas sur le territoire belge, sans préjudice d'une collaboration directe avec des opérateurs de réseaux de communications électroniques et des fournisseurs de services de communications électroniques étrangers, le procureur du Roi peut, par l'intermédiaire du service de police désigné par le Roi, demander à une autorité compétente étrangère d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées, traitées ou transmises au moyen de ce système[1488]. Cette préservation de données « internationales » peut se faire dans l'attente de soumettre une demande d'entraide judiciaire à cette autorité étrangère[1489].

1480. Selon le rapport explicatif de la Convention de Budapest, comme nous le verrons dans le cadre de la mesure d'identification, l'expression « en sa possession » ou « sous son contrôle » est définie en référence à d'une part, la possession matérielle des données et d'autre part, des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un cloud qu'il met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition (« Rapport explicatif de la Convention sur la cybercriminalité », Conseil de l'Europe, Budapest, 23 novembre 2001, § 173).
1481. CICr, art. 39*ter*, § 1, al. 1er.
1482. *Ibid.*, art. 39*ter*, § 1, al. 2.
1483. *Ibid.*, art. 39*ter*, § 1, al. 3 et § 2.
1484. *Ibid.*, art. 39*ter*, § 2.
1485. *Ibid.*, art. 39*ter*, § 3, al. 1er.
1486. Le montant des peines d'amende doit être multiplié par les « décimes additionnels ». Les décimes additionnels sont un coefficient qui s'élève actuellement à huit.
1487. CICr, art. 39*ter*, § 3, al. 2.
1488. *Ibid.*, art. 39*quater*, § 1er. Cette disposition transpose l'article 29 de la Convention de Budapest. Le législateur précise à ce propos créer un cadre légal « pour une collaboration directe avec des ISP étrangers conformément aux pratiques existantes » (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n°54-1966/001, p. 30). A ce propos, voy. V. FRANSSEN et S. TOSZA, *op. cit.*, p. 231.
1489. CICr, art. 39*quater*, § 1er. Cette disposition transpose l'article 29 de la Convention de Budapest. Le législateur précise à ce propos créer un cadre légal " pour une collaboration directe avec des ISP étrangers conformément aux pratiques existantes ». Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n°54-1966/001, p. 30. A ce propos, voy. V. FRANSSEN et S. TOSZA, *op. cit.*, p. 231.

À ce propos, considérant que le processus d'entraide judiciaire actuel est trop lent et lourd, l'Union européenne projette d'adopter des mesures visant à faciliter l'accès aux preuves électroniques comme les courriers électroniques ou les documents se trouvant sur le *cloud*, et ce, quel que soit le lieu de la localisation des données. En ce sens, une proposition de règlement[1490] et de directive[1491] a été déposée le 17 avril 2018. Celles-ci comprennent différents volets, dont la création d'une injonction européenne de production[1492]. Ces textes visent aussi à empêcher l'effacement de données au moyen d'une injonction européenne de conservation[1493], à mettre en place des garanties et des voies de recours tant pour les personnes concernées que pour les prestataires de services, à obliger les prestataires de services à désigner un représentant légal sur le territoire de l'Union et à procurer une sécurité juridique aux entreprises et aux prestataires de services en instaurant un cadre légal identique pour ordonner la fourniture de preuves électroniques. Le Groupe Article 29 a cependant émis des doutes quant à la compatibilité de ces propositions avec l'acquis de l'Union en matière de protection des données, compte tenu de la jurisprudence récente de la Cour de justice de l'Union européenne[1494]. En parallèle aux travaux de l'Union européenne, le Conseil de l'Europe projette également de rédiger un protocole additionnel à la convention de Budapest en vue de favoriser une coopération internationale en matière de cybercriminalité et de preuves ; ce projet faisant encore l'objet de profondes discussions en raison des difficultés juridiques qu'il suscite[1495].

1490. Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, Strasbourg, le 17 avril 2018, COM(2018) 225 final, 2018/0108(COD).
1491. Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, Strasbourg, le 17 avril 2018, COM/2018/226 final – 2018/0107 (COD).
1492. Il s'agira de permettre à une autorité judiciaire d'un État membre de demander des preuves électroniques (telles que des courriels, des SMS ou des messages échangés dans des applications) directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données ; ce prestataire sera alors tenu de répondre dans un délai de 10 jours, et dans les 6 heures en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire).
1493. Cela permettra à une autorité judiciaire d'un État membre de contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données afin que ladite autorité puisse demander ces informations ultérieurement par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production.
1494. Groupe 29, « Statement on e-evidence », 29 novembre 2017. Celui-ci relève notamment que l'ordre de production envisagé vis-à-vis d'organisations qui ne sont pas établies dans l'UE pourrait augmenter le risque d'adoption par des pays non membres de l'UE d'instruments similaires conflit direct avec la législation européenne en matière de protection des données.
1495. A ce propos, voy. le programme relatif à la Conférence Octopos se déroulant du 11 au 13 juillet 2018 : Comité de la Convention sur la cybercriminalité (T-CY), Elaboration d'un 2ème protocole additionnel à la Convention de Budapest sur la cybercriminalité, « Guide de discussions pour les consultations avec la société civile, les autorités chargées de la protection des données et l'industrie », Conseil de l'Europe, Strasbourg, 21 mai 2018, disponible à l'adresse suivante : https ://rm.coe.int/t-cy-2018-16-fr-pdp-consultations-paper/16808af6db<.

ii. L'identification

Afin d'imputer à quelqu'un un accès frauduleux à un système informatique ou une utilisation abusive de données à caractère personnel, il peut s'avérer essentiel de procéder à l'identification d'un utilisateur de services de communications électroniques. À cette fin, le procureur du Roi peut requérir le concours des opérateurs et fournisseurs de communications électroniques tels Base, Orange, Proximus mais aussi des services dits « over the top » tels WhatsApp, Viber, Facebook afin qu'ils fournissent certaines informations telles que celles relatives à une ligne téléphonique, une adresse de courrier électronique, une adresse IP, un code IMEI d'un téléphone[1496] voire l'adresse MAC d'un ordinateur[1497]. Dans le cas où l'infraction n'est pas de nature à emporter une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde[1498], le procureur du Roi ne peut requérir que les données d'identification conservées depuis six mois à partir de sa décision[1499].

iii. La saisie de données informatiques et la recherche dans un système informatique

En cas d'atteinte malveillante à un système informatique, l'officier de police judiciaire peut estimer nécessaire de devoir effectuer une recherche dans ce système, c'est-à-dire « lire, inspecter ou examiner des données »[1500]. Il peut agir immédiatement sans devoir disposer de l'autorisation du procureur du Roi, pour autant que le support soit saisi et qu'il agisse « sans but secret », c'est-à-dire après avoir informé la personne concernée de la fouille effectuée[1501]. Si le système est verrouillé par un code d'accès ou qu'il est chiffré,

1496. *International Mobile Equipment Identity.* L'IMEI est un numéro permettant d'identifier de manière unique les terminaux d'un téléphone mobile. Toute personne peut l'obtenir en composant le code : « *#06# » sur le clavier de son téléphone portable.

1497. L'adresse MAC est un identifiant stocké dans une carte réseau ou une interface réseau stockée dans l'ordinateur. Elle permet de se connecter au routeur d'un réseau *(CICr, art. 46bis). Voy.* J. KERKHOFS et P. VAN LINTHOUT, « L'article 46*bis* du Code d'instruction criminelle et l'obligation de motivation : *de minimis non curat praetor* ? », *T. Strafr.*, 2011/6, pp. 426-431.

1498. Ce seuil comprend un nombre important d'infractions. A titre illustratif, le vol simple est punissable d'une peine d'emprisonnement d'un mois à cinq ans et d'une peine d'amende de vingt-six à cinq cents euros (Code pénal, art. 463).

1499. CICr, art. 46*bis*, § 1er, dernier alinéa. Ces données doivent être fournies « en temps réel » sous peine d'une peine d'amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel (CICr, art. 46*bis*, § 2 et s.).

1500. Rapport explicatif de la Convention de Budapest, § 191.

1501. Selon les travaux parlementaires, la distinction entre « secret » et « non secret » dépend premièrement, de l'intention des enquêteurs « de prendre connaissance des communications ou des données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique ». (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n°54-1966/001, p. 54.) Deuxièmement, le caractère non secret découle de l'obligation faites aux autorités de notifier « dans les plus brefs délais » au « responsable du système informatique » la recherche ou son extension, sauf si son identité ou son adresse ne peut « raisonnablement » être trouvée (CICr, art. 39*bis*, § 7).

l'enquêteur ne peut faire usage de « fausses clés »[1502] ou installer des « dispositifs techniques dans les systèmes informatiques concernés en vue de décryptage et du décodage de données stockées, traitées ou transmises par ce système » sans disposer de l'autorisation du procureur du Roi[1503]. Dans l'hypothèse où le support n'est pas saisi mais pourrait l'être, par exemple, si l'ordinateur est situé dans un cybercafé ou si l'enquête se déroule dans une entreprise et que l'enquêteur n'estime pas nécessaire de devoir emporter les supports, l'officier de police judiciaire doit requérir l'autorisation du procureur du Roi pour pénétrer dans le système informatique[1504]. Dans un cas comme dans l'autre, avant d'entamer la recherche, l'enquêteur est tenu de couper les liaisons externes en activant, par exemple, le mode avion du téléphone[1505]. Ainsi, des informations circulant par des services types WhatsApp, Viber, Hotmail, Gmail ou Facebook ne seront donc pas directement accessibles aux enquêteurs à moins d'être stockées et accessibles « hors connexion »[1506].

Une fois la recherche effectuée, l'enquêteur peut saisir les données et les copier sur un support appartenant aux autorités ou sur des supports disponibles pour des personnes autorisées à utiliser ledit système, et ce, en cas d'urgence ou pour des raisons techniques[1507]. Dans le cas où la copie n'est pas possible en raison d'un volume trop important ou pour des raisons techniques, le procureur du Roi peut, à l'aide de moyens techniques appropriés, se limiter à empêcher l'accès aux données saisies et à leurs copies tout en s'assurant à nouveau de leur intégrité[1508]. Par ailleurs, les données peuvent être rendues inaccessibles ou, après en avoir pris copies, être retirées si les données « forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes ». Il s'agira, par exemple, de prendre copie d'images pédopornographiques tout en les effaçant du lieu où elles sont stockées[1509]. *In fine,* le procureur du Roi est tenu de fournir au responsable du système informatique un résumé des données copiées, rendues inaccessibles ou reti-

1502. Il s'agit de « tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès – sous forme lisible – aux données contenues dans ce système » (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n°54-1966/001, p. 22).

1503. CICr, art. 39*bis*, § 5.

1504. *Ibid.*, art. 39*bis*, § 2.

1505. *Ibid.*

1506. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n°54-1966/001, p. 17.

1507. CICr, art. 39*bis*, § 6.

1508. F. ROGGEN, « L'extension des moyens d'investigation et des mesures de contrainte en procédure pénale », *R.G.C.F.*, 2003/5, p. 113. Notons que dans un arrêt du 22 octobre 2013, la Cour de cassation dit pour droit que la saisie de données informatiques est une base légale suffisante pour le blocage de site Internet, étendant ainsi la portée de l'article 39*bis* CICr. En effet, l'article précité ne vise pas, à notre sens, le blocage de site Internet au stade de l'information. A cet égard voy. R. SCHOEFS, « Changement de méthode dans la lutte contre The Pirate Bay : la saisie de données autorisée », *T. Strafr.*, 2014/2, pp. 131-142 (note sous Cass., 22 oct. 2013, P.13.0550.N et P.13.0551.N) ; P. MONVILLE, et M. GIACOMETTI, « Les fournisseurs d'accès à Internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014/2, n° 55, pp. 68-76 ; C. FORGET (sous la direction de J.-F. HENROTTE et F. JONGEN), « La collecte de preuves informatiques en matière pénale » in *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, pp. 260 et s.

1509. *Doc. Parl.*, Ch. repr., sess. ord., 1999-2000, n° 50-213/1, *pp. 20-21.*

rées[1510]. Ce document devrait lui permettre d'exercer un recours dans les conditions prévues par l'article 28*sexies* CICr et d'exiger la levée d'un acte d'enquête pour autant qu'il démontre « être lésé » par cette mesure.

iv. Le blocage de site Internet

En 2018, le Centre pour la Cybersécurité Belgique annonçait avoir réussi à bloquer en moyenne quatre sites Internet frauduleux par jour, soit au total 1478 sites Internet[1511]. Ce blocage de sites Internet effectué notamment suite à une dénonciation d'internautes, via le site suspect@safeonweb.be, vise à lutter contre les attaques de phishing grâce à une collaboration des quatre principaux navigateurs : Google Chrome, Mozilla Firefox, Safari et Internet Explorer. À défaut de leur collaboration, le CCB pourrait également solliciter l'intervention du procureur du Roi lequel dispose des compétences nécessaires pour ordonner le blocage d'un site Internet. Cette mesure d'enquête n'est toutefois pas spécifiquement réglementée par le Code d'instruction criminelle,[1512] mais est incluse dans l'article 39*bis* CICr, soit l'article régissant la saisie de données informatiques[1513]. Cette disposition permet en effet au procureur du Roi d'empêcher l'accès aux données si leur copie s'avère impossible[1514] ou afin de garantir l'intégrité des données[1515] et effectuer une sorte de « mise sous scellés »[1516]. Comme déjà précisé *supra*, les données formant l'objet de l'infraction, produites par l'infraction ou contraires à l'ordre public et aux bonnes mœurs ou risquant d'endommager le système informatique – un virus par exemple – peuvent également être rendues inaccessibles et retirées du système informatique[1517].

1510. CICr, art. 39*bis*, § 5.
1511. CCB, 1500 faux sites Internet bloqués grâce à suspect@safeonweb.be, consulté le 05/09/2019, disponible à l'adresse suivante : https ://www.cert.be/fr/news/1500-faux-sites-Internet-bloques-grace-suspect-safeonwebbe.
1512. D'autres lois particulières encadrent l'effacement ou le retrait de données. Il s'agit par exemple des articles 39 et 41 de la loi sur la protection de la vie privée. Ces dispositions permettent au juge d'ordonner l'effacement de données à caractère personnel traitées en violation de la loi sur la protection de la vie privée. De même, les fournisseurs de services Internet peuvent être tenus de supprimer les données traitées en violation de la LVP sur base d'une décision du président du tribunal de première instance en vertu des articles 12 et 14 de la LVP. Voy. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993. En outre, en matière de droits de propriété intellectuelle, la personne préjudiciée peut également agir par le biais d'une action en cessation (Code de droit économique, art. XI.334. § 1er).
1513. Dans le cadre de l'arrêt « Piratebay », la Cour de cassation a dit pour droit que le blocage de site Internet entre dans le champ d'application de la saisie de données informatiques (voy. À ce propos : R. SCHOEFS, « Changement de méthode dans la lutte contre The Pirate Bay : la saisie de données autorisée », *T. Strafr.*, 2014/2, pp. 131-142, note sous Cass., 22 oct. 2013, P.13.0550.N et P.13.0551.N ; P. MONVILLE, et M. GIACOMETTI, « Les fournisseurs d'accès à Internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014/2, n° 55, p. 68-76).
1514. CICr, art. 39*bis*, § 6.
1515. *Ibid.*.
1516. O. KLEES, F. ROGGEN, D. VANDERMEERSCH, « Les saisies en matière pénale et référé pénal », in *Droit pénal et procédure pénale*, Malines, Kluwer, 2006, p. 71. F. ROGGEN, « L'extension des moyens d'investigation et des mesures de contrainte en procédure pénale », *R.G.C.F.*, 2003/5, p. 113.
1517. CICr, art. 39*bis*, § 6.

À toutes fins utiles, indiquons que, vu l'ingérence que comporte une telle mesure pour le droit à la liberté d'expression, il est regrettable que, conformément à la jurisprudence de la Cour européenne des droits de l'Homme[1518], cette mesure ne soit pas strictement encadrée par la loi.

c) Les actes d'enquête au stade de l'instruction

Les méthodes d'enquête au stade de l'instruction entraînent une ingérence plus importante dans les droits et libertés des personnes concernées et relèvent dès lors de la compétence du juge d'instruction lequel peut requérir les officiers de police judiciaire en ce inclus les inspecteurs du CSIRT. On précisera néanmoins que l'obligation de collaboration ne peut être dévolue aux membres du service d'inspection du CSIRT, cette disposition visant uniquement les officiers de police judiciaire auxiliaires du procureur du Roi.

i. Le repérage

Le repérage peut s'avérer essentiel en cas d'attaque malveillante sur un système, puisqu'il permet de procéder « au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées » ou à « la localisation de l'origine ou de la destination de communications électroniques »[1519]. Autrement dit, le juge d'instruction peut isoler cer-

1518. Dans un arrêt du 18 décembre 2012, la Cour européenne des droits de l'Homme se prononce sur une mesure de blocage de site Internet prise par un tribunal. Ce dernier avait ordonné de bloquer l'accès à « Google sites » afin d'empêcher l'accès à un site Internet dont le propriétaire était poursuivi pour outrage à la mémoire d'Atatürk. Le requérant, personne tierce à la procédure, invoquait la violation du droit à la liberté d'expression, celui-ci ne pouvant plus accéder à son propre site Internet alors qu'il n'était pas lié aux poursuites pénales entamées. La Cour constate la violation de l'article 10 de la CEDH en raison de l'absence de détermination suffisante du cadre légal. De plus, selon la Cour, la procédure n'offre pas de garanties suffisantes contre les risques d'abus et d'arbitraire. (Cour eur. D.H., arrêt HüseyÎn *Yildirim* c. *Turquie*, *n°* 2778/02, 18 décembre 2012). Notons dans le cadre de cet arrêt, l'opinion concordante du juge Pinto De Albuquerque précisant, eu égard aux dispositions de droit international, un ensemble de critères minimaux notamment :
1) une définition des catégories de personnes et d'institutions susceptibles de voir leurs publications bloquées (les propriétaires nationaux ou étrangers de contenus, sites ou plates-formes illicites, les utilisateurs de ces sites ou plates-formes, etc.) ;
2) une définition des catégories d'ordonnances de blocage, par exemple celles qui visent le blocage de sites, d'adresses IP, de ports, de protocoles réseaux, ou le blocage de types d'utilisation, comme les réseaux sociaux ;
3) une disposition sur le champ d'application territoriale de l'ordonnance de blocage ;
4) une limite à la durée d'une telle ordonnance de blocage ;
5) l'indication des « intérêts » justifiant la mesure, du critère de proportionnalité et de nécessité ;
6) la détermination des autorités compétentes pour émettre une ordonnance de blocage motivée ;
7) une procédure à suivre pour l'émission de cette ordonnance, comprenant l'examen par l'autorité compétente du dossier à l'appui de la demande d'ordonnance et l'audition de la personne ou institution lésée, sauf si cette audition est impossible ou se heurte aux « intérêts » poursuivis ;
8) la notification de l'ordonnance de blocage et de sa motivation à la personne ou institution lésée ;
9) une procédure de recours de nature judiciaire contre l'ordonnance de blocage.
1519. CICr, art. 88*bis*, § 1er.

taines données d'appel, comme les différents numéros de téléphone composés ou reçus par un téléphone, leur durée, le moment de la prise de contact, etc.,[1520] et, dès lors, par ce biais localiser le signal émis par un appareil en fonctionnement sans qu'une communication ne soit émise ou reçue[1521] et ainsi, géolocaliser une personne[1522]. Dans certaines situations spécifiques de flagrant délit[1523], le procureur du Roi peut également ordonner un tel dispositif. En effet, c'est parce que le délit se commet ou vient de se commettre que la mesure doit « permettre immédiatement la constatation de [l'] infraction et la recherche des preuves qui permettront une meilleure appréciation du juge du fond »[1524]. La disposition ne vise toutefois que les officiers de police judiciaire auxiliaires du procureur du Roi excluant dès lors les membres du service d'inspection du CSIRT.

ii. La recherche et l'extension de recherche dans un système informatique

Après avoir effectué une recherche dans un système informatique, le juge d'instruction peut autoriser l'extension de cette recherche vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée. Cette extension doit, d'une part, être nécessaire à la manifestation de la vérité et ne peut, d'autre part, être réalisée que s'il s'avère que d'autres mesures seraient disproportionnées ou s'il existe un risque de perdre certains éléments de preuve[1525]. En outre, afin d'éviter une

1520. A noter que *l'accès aux données de trafic et de* localisation conservées par les opérateurs sur base de l'article 126 de la loi du 13 juin 2005, soit l'obligation de conservation des métadonnées est limité aux données stockées depuis six mois pour les infractions punies d'un à cinq ans d'emprisonnement, neuf mois lorsque l'infraction est de nature à emporter une peine de cinq ans ou plus, douze mois lorsqu'il est question de terrorisme. (CICr, art. 88*bis*, § 2). Ces données doivent être fournies « en temps réel », obligation sanctionnée par une peine d'amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » dont le non-respect est sanctionné dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel (CICr, art. 88*bis*, § 4).

1521. Cass., 24 mai 2011, RG P.11.0909.N, *Pas.*, 2011.

1522. Cette mesure ne peut être ordonnée qu'en présence d'indices sérieux d'infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde et pour autant que sa mise en œuvre s'avère nécessaire à la manifestation de la vérité. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête dans une ordonnance motivée. Cette mesure doit être limitée dans le temps, deux mois maximums à dater de l'ordonnance postérieure ou antérieure sans préjudice de renouvellement (CICr, art. 88*bis*, § 1er et s.).

1523. En cas de flagrant délit, le procureur du Roi peut également ordonner le repérage, pour les infractions visées à l'article 90*ter*, §§ 2 à 4 du CICr avec confirmation de la mesure dans les vingt-quatre heures par le juge d'instruction. En cas d'enquête relative à une infraction terroriste, prise d'otage, détention illégale ou extorsion, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire. Uniquement concernant les infractions terroristes, le procureur du Roi peut ordonner le repérage des communications dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction ne soit nécessaire (CICr, art. 88*bis*, § 1, al. 6 et s.).

1524. M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, 2006, 2e éd., p. 373

1525. CICr, art. 88*ter*, al. 1er.

intrusion illimitée dans les systèmes informatiques, la mesure est limitée aux parties du système auxquelles « les personnes autorisées à l'utiliser » ont spécifiquement accès[1526]. L'autorisation doit être écrite ou orale en cas d'extrême urgence et sous réserve de la confirmer de manière motivée dans les plus brefs délais[1527]. Lorsqu'il s'avère que les données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. En ce cas, le juge d'instruction communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'État concerné, si celui-ci peut raisonnablement être déterminé[1528].

iii. La collaboration dans le cadre d'une enquête dans un système informatique

Le devoir de collaboration peut s'avérer particulièrement utile aux enquêteurs afin de permettre une recherche dans un système informatique ou une saisie de données informatiques. La collaboration peut être exigée de manière « active » (obligation d'agir) ou de manière « passive » (obligation d'information). On précisera que cette compétence ne peut être déléguée qu'aux officiers de police judiciaire auxiliaires du procureur du Roi et ne vise donc pas les membres du service d'inspection du CSIRT.

Le devoir de collaboration active

Le juge d'instruction peut ordonner à « toute personne appropriée » de mettre un système informatique en fonctionnement et de fournir certaines données dans la forme qu'il aura demandée[1529]. Le défaut de collaboration est passible de sanctions pénales[1530] sauf à l'égard de l'inculpé et/ou des personnes visées par l'article 156 CICr[1531] à savoir, les ascendants ou descendants de la personne prévenue ainsi que ses proches, ces dernières ne pouvant donc être tenues à l'obligation de collaborer. L'obligation « d'action » consiste en un « engagement à fournir des efforts », une personne ne pouvant être tenue de déployer des moyens qu'elle est incapable de fournir[1532]. La loi prévoit donc expressément que les

1526. *Ibid.*r, art. 88*ter*, al. 2.

1527. *Ibid.*, art. 88*ter*, al. 5.

1528. *Ibid.*, art. 88*ter*, al. 4.

1529. *Ibid.*, art. 88*quater*, § 2.

1530. Le défaut de collaboration est passible de sanctions pénales à savoir, une peine d'emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement. Cette sanction peut être portée d'un à cinq ans avec une peine d'amende de cinq cents euros à cinquante mille euros dans le cas où la collaboration aurait eu pour effet d'empêcher la commission d'un crime ou d'un délit ou d'en limiter les effets. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel. On précisera que la mesure ne peut porter atteinte au droit au silence et aux règles de droit commun relatives aux personnes tenues au secret professionnel (CICr, art. 88 *quater*, §§ 3-4).

1531. CICr, art. 8 *quater*, § 2, al. 2.

1532. *Doc. parl.*, Ch. repr., 1999-2000, n° 0213/001, *p. 27.*

personnes sont tenues d'y donner suite « dans la mesure de leurs moyens »[1533]. En pratique cependant, l'enquêteur pourra être tenté de détourner cette limite en imposant le concours de tiers en s'appuyant sur une autre base légale telle que l'interception des communications visée par l'article 90*quater* CICr[1534] laquelle ne prévoit pas de limite.

La collaboration passive

La collaboration passive consiste en l'obligation de fournir certaines informations aux enquêteurs, telles que les clés de chiffrement ou un mot de passe afin de leur permettre d'effectuer une recherche dans un système informatique ou une saisie de données informatiques[1535]. Cette obligation peut être adressée sur la base d'une ordonnance motivée du juge d'instruction, aux importateurs de distributeurs d'ordinateurs ou de logiciels, les « *trusted third parties* »[1536], les fournisseurs de services, les opérateurs, les ingénieurs d'entreprises ayant élaboré une configuration informatique spécifique, les spécialistes de la sécurité, etc.[1537]

La loi ne précise pas si l'ordonnance relative à l'obligation de fournir certaines informations peut être adressée à un suspect[1538]. Dans un jugement du 17 novembre 2014, le Tribunal correctionnel de Termonde a rappelé qu'aucun suspect ne peut être obligé de collaborer activement avec les autorités poursuivantes. Il estima qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ils avaient été contraints, moyennant une prestation intellectuelle propre, de contribuer activement à l'administration de la preuve de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité[1539]. Cette approche fut confirmée par la Cour d'appel de Gand[1540]. En effet, le droit au silence ne couvre pas uniquement le droit de se taire mais

1533. CICr, art. 88*quater*, § 2.
1534. L'affaire rendue récemment par la cour d'appel d'Anvers permet d'illustrer notre propos puisqu'une ordonnance du juge d'instruction prise sur base des articles 88*bis* du CICr et 90*quater* du CICr imposait à Skype de collaborer en vue de permettre l'interception des données de communications électroniques. L'entreprise invoquait l'impossibilité matérielle de prêter son concours en raison du chiffrement des données depuis le destinateur et le déchiffrement une fois chez le destinataire. Or, l'article 90*quater* CICr ne souffre d'aucune dérogation à l'obligation de collaboration. Dès lors, selon la cour d'appel, en créant ses services, Skype aurait dû tenir compte des obligations de collaboration découlant du droit national belge. (Anvers, 15 novembre 2017, C.1288.2017, inédit.) Cet arrêt fut soumis à la Cour de cassation mais les éléments précités ne furent pas abordés (Cass., 19 février 2019, P.17.1229.N).
1535. Cette ordonnance peut être prise de manière large à l'égard de « quiconque dont on présume » qu'il a une connaissance particulière du système informatique visé relatives à son fonctionnement ou la manière d'y accéder, par exemple les clés de chiffrement ou les mots de passe (CICr, art. 88*quater*, § 1er)
1536. Un tiers de confiance est une personne physique ou morale habilitée à effectuer des opérations de sécurité tels que l'authentification, la transmission et le stockage.
1537. *Doc. parl.*, Ch. repr., 2015-2016, n° 1966/001, p. 50.
1538. CICr, art. 88*quater*, § 1er.
1539. Corr. Termonde, 17 novembre 2014, *T. Strafr.*, 2016/3, pp. 255-260.
1540. Gand 23 juin 2015, *NjW*, 2016, liv. 336, p. 134, note C. CONINGS.

englobe également le droit de ne pas devoir fournir des informations susceptibles d'affecter substantiellement la position de l'accusé ou de favoriser une incrimination »[1541]. Récemment toutefois, la Cour d'appel d'Anvers (chambre des mises en accusation) a considéré que l'ordonnance d'un juge d'instruction imposant à un inculpé de dévoiler le code pin de son téléphone portable sous peine de sanctions pénales n'était pas incompatible avec les exigences du droit à un procès équitable[1542]. Cette dernière considère en effet que la clé de chiffrement n'est pas en soi incriminante mais ce sont les données stockées dans le système informatique qui peuvent l'être. De plus, le juge fait mention du fait que la loi ne prévoit pas une telle dérogation, et ce, conformément à l'arrêt *Saunders* de la Cour européenne des droits de l'homme, arrêt auquel s'est par ailleurs référé le législateur dans les travaux préparatoires[1543]. Dans cette décision, la juridiction de Strasbourg effectue une distinction entre les données recueillies « au mépris de la volonté du suspect » et les données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais « qui existent indépendamment de sa volonté » telles des documents recueillis sur la base d'un mandat, des empreintes digitales, haleine, sang, urine[1544]. Selon la Cour européenne, cette dernière catégorie n'entre pas dans le champ d'application du droit au silence[1545]. En tout état de cause, la chambre des mises en accusation estime que le droit au silence n'est pas d'un droit absolu. En l'espèce et en application du principe de proportionnalité, elle estime que l'ingérence ne peut être qualifiée de grave et qu'elle se justifie dans l'intérêt public[1546].

L'analyse critique de cet arrêt dépasserait le cadre de cette contribution[1547]. Soulignons toutefois que l'on pourrait soutenir qu'à la différence de documents fiscaux tenus en vertu d'une obligation légale et saisissable dans le cadre d'une perquisition, un mot de passe peut être créé sur initiative de son auteur et devrait donc, en ce cas, être couvert par le

1541. Cour EDH, *Saunders* c. *Royaume-Uni*, n° 19187/91, CEDH 1996-VI.
1542. Anvers, 21 décembre 2017, chambre des mises en accusation, K/2895/2017, *inédit*. Dans la foulée, la Cour d'appel de Gand (chambre des mises en accusation) a rendu une décision similaire estimant qu'il s'agissait d'une obligation de collaboration passive. Voy. Gand, 16 janvier 2018. KI2018/22/2, *inédit*.
1543. *Doc. parl.*, Ch. repr., 1999-2000, n° 0213/001, *p. 27*.
1544. Cour EDH, *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, § 69.
1545. *Ibid.*
1546. La validité de cette distinction a été critiquée dans une opinion dissidente. Il y était relevé que : « Pour quelle raison un suspect aurait-il le droit de ne pas subir de pressions pour l'obliger à faire des déclarations l'incriminant, mais pourrait-il être forcé à coopérer pour fournir des données à charge ? La nouvelle raison d'être adoptée par la Cour ne justifie pas cette distinction puisque dans les deux cas, la volonté du suspect n'est pas respectée : en effet, il est contraint de participer à sa propre condamnation. De plus, le critère utilisé pour établir la distinction n'est pas sans poser de problème. Peut-on vraiment dire que le contenu d'un ballon d'alcootest dans lequel une personne soupçonnée de conduite en état d'ivresse a été contrainte de souffler a une existence indépendante de la volonté du suspect ? Que dire d'un code PIN ou de la clé d'un système de chiffrement, enfouis dans la mémoire du suspect ? ». Cour EDH, *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, opinion dissidente du juge Martens à laquelle le juge Kuris déclare se rallier, I. C.12.
1547. Pour un approfondissement voy. C. CONINGS, « U hebt het recht te zwijgen. Uw login kan en zal tegen u worden gebruikt ? Over ontsleutelplicht, zwijgrecht en 'nemo tenetur' », *N.C.*, n° 5, 2018, pp. 457-472.

droit au silence[1548]. En revanche, dans certaines situations, un mot de passe consiste en un système d'authentification par empreinte digitale ou encore par reconnaissance faciale. En ce cas, la collaboration pourrait être due considérant que les données existent indépendamment de la volonté de l'auteur. Insistons toutefois sur le fait que, dans ce dernier cas, si les autorités doivent contraindre physiquement le suspect à collaborer, le recours à des pouvoirs coercitifs ne peut se faire à n'importe quel prix. Pour examiner la compatibilité d'un tel dispositif avec le droit au silence, la Cour européenne des droits de l'homme examine tour à tour les facteurs suivants : la nature et le degré de la coercition employée pour l'obtention des éléments de preuve ; le poids de l'intérêt public à la poursuite de l'infraction en question et à la sanction de son auteur ; l'existence de garanties appropriées dans la procédure et l'utilisation faite des éléments ainsi obtenus[1549]. Enfin, concernant les sanctions pénales, on peut se demander quelles seraient les conséquences d'un défaut de collaboration en cas d'oubli du mot de passe ou d'absence de conservation de la clé de chiffrement laquelle n'est imposée par aucune obligation légale. En effet, comme souligné *supra*, si le Code d'instruction criminelle précise que les personnes sont tenues de donner suite à l'ordonnance relative à l'obligation d'agir « dans la mesure de leurs moyens »[1550], l'obligation d'information ne souffre d'aucune dérogation[1551].

1548. Cour EDH, *Funke c. France*, 25 février 1993, n° 110588/83. Notons qu'en France, une telle obligation a été validée par le Conseil constitutionnel considérant que « Les dispositions critiquées n'imposent à la personne suspectée d'avoir commis une infraction, en utilisant un moyen de cryptologie, de délivrer ou de mettre en œuvre la convention secrète de déchiffrement que s'il est établi qu'elle en a connaissance. Elles n'ont pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées. En outre, l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit. Enfin, ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée. ». Voy. Décision n° 2018-696 du Conseil Constitutionnel, QPC du 30 mars 2018, *J.O.R.F.*, n°0076 du 31 mars 2018, texte n° 111 (ECLI :FR :CC :2018 :2018.696.QPC).

1549. Cour EDH, *Jalloh c. Allemagne*, 11 juillet 2006, n° 54810/00, § 117.

1550. CICr, art. 88*quater*, § 2.

1551. En ce sens, la directive relative à la présomption d'innocence et au droit d'assister à son procès dans le cadre des procédures pénales précise : « L'exercice du droit de ne pas s'incriminer soi-même ne devrait pas empêcher les autorités compétentes de réunir les preuves que l'on peut obtenir légalement du suspect ou de la personne poursuivie en recourant à des pouvoirs de contrainte licites et qui existent indépendamment de la volonté du suspect ou de la personne poursuivie, tels que des documents recueillis en vertu d'un mandat, des documents pour lesquels est prévue une obligation légale de conservation et de production sur demande, les échantillons d'air expiré, de sang et d'urine ainsi que les tissus corporels en vue d'une analyse de l'ADN ». Cette directive requiert donc a priori un lien entre la production sur demande et l'obligation de conservation de données ce qui n'est pas le cas pour un mot de passe. Considérant 29 de la directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, *J.O.U.E.*, L 65, 11 mars 2016, pp. 1–11.

D. La clôture de l'enquête et le pouvoir de sanctions

1. Les pouvoirs de sanctions de l'APD

Une fois l'enquête terminée, l'inspecteur général et les inspecteurs de l'APD rédigent leur rapport et le joignent au dossier[1552]. Lorsque les faits font état d'une infraction pénale, un procès-verbal de constat d'infraction est rédigé[1553]. L'inspecteur général peut alors décider de transmettre le dossier au président de la chambre contentieuse ou de le transmettre au procureur du Roi[1554]. En l'absence d'infraction, il peut décider de classer le dossier sans suite[1555]. S'il estime que l'Autorité de protection des données n'est pas compétente, il peut également transmettre les informations à une autorité de protection des données d'un autre État[1556].

De son côté, la chambre contentieuse a le pouvoir de : classer le dossier sans suite ; ordonner le non-lieu ; prononcer la suspension du prononcé ; proposer une transaction ; formuler des avertissements et des réprimandes ; ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits ; ordonner que l'intéressé soit informé du problème de sécurité ; ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ; ordonner une mise en conformité du traitement ; ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ; ordonner le retrait de l'agréation des organismes de certification ; donner des astreintes ; donner des amendes administratives ; ordonner la suspension des flux transfrontières de données vers un autre État ou un organisme international ; transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informera des suites données au dossier ; décider au cas par cas de publier ses décisions sur le site Internet de l'Autorité de protection des données[1557]. La publication des décisions peut constituer une « sanction redoutable » pour le responsable du traitement ou le sous-traitant concerné, cette dénonciation étant susceptible d'avoir des incidences sur leur réputation[1558].

Les amendes administratives peuvent s'élever de deux cent cinquante euros à quinze mille euros jusqu'à vingt mille euros[1559]. L'article 83, al. 5, du RGPD indique par ailleurs que les montants peuvent s'élever jusqu'à vingt millions d'euros ou quatre pour cent du chiffre d'affaires annuel mondial d'une entreprise considérant que les sanctions doivent s'avérer

1552. Loi sur l'APD, art. 91, § 1er.

1553. *Ibid.*, art. 67, § 1er.

1554. *Ibid.*, art. 91, § 2.

1555. *Ibid.*, art. 91, § 2.

1556. *Ibid.*, art. 91, § 2.

1557. *Ibid.*, art. 100.

1558. C. De Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politéia, 2019, p. 150.

1559. Voy. les articles 222 à 227 de la loi du 30 juillet 2018.

« effectives, proportionnées et dissuasives »[1560]. On précisera que cette disposition ne s'applique pas à l'égard des autorités publiques, de leurs préposés ou mandataires[1561], ce qui pourrait être source de discrimination par rapport au secteur privé[1562]. Les décisions de la chambre contentieuse peuvent faire l'objet d'un recours dans un délai de trente jours, à compter de la notification à la Cour des marchés qui traite l'affaire selon les formes du référé[1563]. Les décisions sont néanmoins exécutoires par provision, nonobstant recours, sauf exception prévues par la loi ou sauf si la chambre contentieuse en décide autrement[1564]. Cette disposition ne s'applique pas à l'égard des décisions d'effacement des données[1565].

Des amendes pénales sont également prévues aux articles 222 à 230 de la loi du 30 juillet 2018 dont les montants sont fixés, pour la plupart, entre deux cent cinquante euros et quinze mille euros. La loi ne prescrit donc aucune peine d'emprisonnement. Compte tenu de la possibilité d'imposer à la fois des sanctions administratives et des sanctions pénales pour un même comportement, l'autorité de contrôle compétente et le Collège des procureurs généraux peuvent conclure un protocole régissant les accords de travail[1566]. Ce protocole devrait permettre d'éviter de contrevenir au principe du *non bis in idem*[1567] en vertu duquel on ne peut sanctionner deux fois un comportement infractionnel ayant déjà donné lieu à une décision définitive[1568].

Quoi qu'il en soit, lorsque l'inspecteur général a transmis le dossier au procureur du Roi et que le ministère public renonce à engager des poursuites pénales, à proposer une résolution à l'amiable ou une médiation pénale au sens de l'article 216*ter* du Code d'instruction criminelle, ou lorsque le ministère public n'a pas pris de décision pendant un délai de six mois à compter du jour de réception du dossier, l'Autorité de protection des données peut décider de rouvrir la procédure administrative[1569].

1560. RGPD, art. 83, al. 1er.
1561. Loi du 30 juillet 2018, art. 221, § 2.
1562. Cette différence de traitement fait actuellement l'objet d'un recours à la Cour constitutionnelle. Voy. C. De Terwangne, E. Degrave, A. Delforge et L. Gerard, *op. cit.*, Bruxelles, Politéia, 2019, p. 151.
1563. Loi sur l'APD, art. 108, § 1, 1°.
1564. *Ibid.*, art. 108, § 1, 2°.
1565. *Ibid.*, art. 108, § 1, 3°.
1566. Loi du 30 juillet 2018, art. 229, § 1er.
1567. En ce sens le considérant 149 du RGPD précise : « L'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe *ne bis in idem* tel qu'il a été interprété par la Cour de justice. ».
1568. Ce principe garanti par l'article 4 du Protocole n°7 à la Convention européenne des droits de l'Homme s'applique en matière pénale. Il peut également trouver à s'appliquer pour des sanctions administratives en application des « critères Engels » c'est-à-dire, la qualification de l'infraction en droit national, la nature de l'infraction et le degré de gravité de la sanction infligée. L'objectif est d'éviter qu'une personne puisse être poursuivie sans bénéficier des protections découlant d'une procédure pénale au motif d'être qualifiée de procédure administrative par le législateur par exemple. (Cour EDH, *Engel et al. c. Pays-Bas*, 8 juin 1976, série A, n°22.)
1569. Loi sur l'APD, art. 91, § 3.

2. Les pouvoirs de sanctions NIS

En cas de constat de manquements aux exigences imposées par la loi, le service d'inspection peut mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique concerné de se conformer, dans un délai qu'il fixe, aux obligations qui lui incombent[1570]. Au préalable néanmoins, le service d'inspection informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure[1571]. Le contrevenant dispose alors d'un délai de quinze jours pour formuler par écrit ses moyens de défense et peut demander à être d'entendu[1572]. En cas de non-respect dans le délai fixé de la mise en demeure, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection. Ce procès-verbal est adressé à l'autorité sectorielle compétente[1573].

La violation des dispositions prévues par la loi NIS est passible de sanctions administratives et de sanctions pénales. Nous ne les détaillons pas ici dans la mesure où elles ont déjà été exposées dans le chapitre XX de cet ouvrage.

3. Les pouvoirs de sanctions des juridictions pénales

Au terme de l'enquête pénale, le procureur du Roi est tenu de décider s'il est raisonnable, utile, voire opportun, d'exercer ou non l'action publique[1574]. À cette fin, il peut, sur la base des renseignements dont il dispose, notamment : classer l'affaire sans suite[1575], citer directement une personne devant le tribunal de police[1576] ou correctionnel[1577], la convoquer par procès-verbal[1578], proposer l'application de la procédure de reconnaissance préalable de la culpabilité[1579], proposer une transaction pénale[1580] ou encore proposer une médiation pénale[1581].

En cas de renvoi devant les juridictions pénales, le juge constatant la violation d'une infraction, peut infliger une peine principale accompagnée ou non d'une peine accessoire.

1570. Loi NIS, art. 48, § 1er.
1571. *Ibid.*, art. 48, § 2.
1572. *Ibid.*, art. 48, § 3.
1573. *Ibid.*, art. 49, § 1er.
1574. M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale*, Bruxelles, Éditions Larcier, 2012, p. 265.
1575. Il s'agit d'une pratique administrative permettant au procureur du Roi de classer l'affaire sans suite soit car il ne dispose pas d'indices suffisants, soit pour des raisons d'opportunité. Le plaignant dispose toujours de la possibilité de citer directement devant le tribunal ou de se constituer partie civile entre les mains du juge d'instruction ou encore d'introduire une action devant le tribunal civil.
1576. CICr, art. 145.
1577. *Ibid.*, art. 182.
1578. *Ibid.*, art. 216*quater*.
1579. *Ibid.*, art. 216. Cette procédure est introduite dans le Code d'instruction criminelle suite à l'adoption de la loi du 5 février 2016.
1580. CICr, art. 216*bis*.
1581. *Ibid.*, art. 216*ter*.

La violation des règles relatives à la protection des données est passible de peines correctionnelles strictement prévues par la loi. Nous renvoyons toutefois le lecteur à ce qui a été précisé ci-devant, mais aussi à la partie relative au droit pénal matériel de cet ouvrage où sont détaillées par infractions les peines qui y sont assorties[1582].

E. Les règles relatives à la protection des données

1. Principes généraux

Une administration publique, telle que l'APD ou encore une autorité NIS, est soumise aux règles du RGPD lorsqu'elle traite des données à caractère personnel[1583] et au titre I de la loi du 30 juillet 2018. Concernant la base de licéité du traitement, la loi en question prévoit que le traitement de données à caractère personnel par le CSIRT[1584], constitue un intérêt légitime du responsable du traitement concerné. Il en est *a fortiori* de même pour l'APD même si la loi ne l'indique pas expressément.

En revanche, les autorités policières et judiciaires, lorsqu'elles traitent des données à des fins de prévention et détection des infractions pénales ou dans le cadre d'enquête et des poursuites en la matière[1585], sont soumises aux règles fixées par la directive 2016/680[1586]. Cette directive, transposée dans le titre 2 de la loi du 30 juillet 2018[1587], encadre les traitements de données à des fins pénales par les « autorités compétentes », c'est-à-dire, toute « autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales » ainsi que « tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique »[1588]. Le champ d'application de la directive 2016/680 est donc déterminé à la fois par la finalité répressive poursuivie par le responsable du traitement et par sa qualité « d'autorité compétente » telle que définie par la loi. On précisera que la directive inclut également dans son champ d'application les activités de police dans le cadre des règles de sanctions de droit administratif pour autant qu'elles recouvrent un caractère « pénal » au sens de la jurisprudence de la Cour de justice de l'Union européenne[1589], c'est-à-dire, lorsque ces sanctions administratives recouvrent un caractère « punitif et dissuasif »[1590].

Compte tenu de cette définition, on pourrait considérer que les inspecteurs des services d'inspection sectoriel ou les inspecteurs de l'APD doivent se soumettre au respect de la directive 2016/680, les premiers pouvant avoir la qualité d'officier de police judiciaire[1591], les seconds ayant des missions pouvant recouvrir un caractère répressif[1592]. Toutefois, le législateur national délimite davantage le champ d'application du titre 2 de la loi du 30 juillet 2018 que ne le prévoit la directive 2016/680, celui-ci énumérant exhaustivement les différentes « autorités compétentes » visées dans ce cadre[1593]. Ainsi, l'article 26, 7°, de la loi du 30 juillet 2018 stipule qu'il s'agit : des services de police, des autorités judiciaires, c'est-à-dire les cours et tribunaux du droit commun et le ministère

1582. Voy. dans le présent ouvrage la contribution de Valéry VANDER GEETEN sur le *hacking* éthique (Chap. 5).
1583. C. DE TERWANGNE, « Titre 2 – Définitions clés et champ d'application du RGPD » in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie,* sous la coordination de K. ROSIER et C. DE TERWANGNE, Bruxelles, Larcier, 2018, pp. 70 et *s.*
1584. Selon le considérant 29 du RGPD, il s'agit de « la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité, constitue un intérêt légitime du responsable du traitement concerné. »
1585. Plus précisément, la finalité expressément prévue par la directive est la « prévention et détection des infractions pénales, les enquêtes et poursuites en la matière ainsi que l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données ». (Directive 2016/680, art. 1 et Loi du 30 juillet 2018, art. 27).
1586. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *O.J. L 119,* 4 mai 2016, pp. 89–131 (ci-après « directive 2016/680 »).
1587. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
1588. Directive 2016/680, art. 3, § 7.
1589. *Ibid.*, consid. 13. Cette interprétation autonome et indépendante du droit des États membres, vise à assurer une interprétation uniforme du droit de l'Union. En effet, comme le souligne la C.J.U.E. à l'égard du respect de la règle *ne bis in idem* : « Même en l'absence d'harmonisation des législations pénales des États membres, l'application uniforme du droit de l'Union requiert, selon une jurisprudence constante, qu'une disposition ne renvoyant pas au droit de ces États reçoive une interprétation autonome et uniforme, qui doit être recherchée en tenant compte du contexte de la disposition dans laquelle elle s'insère et de l'objectif poursuivi ». (C.J.U.E., 27 mai 2014, *Zoran Spasic* C129/14 PPU, point 79).
1590. Ces critères ont notamment été retenus par la CJUE à l'égard de la reconnaissance mutuelle des sanctions pécuniaires infligées en cas d'infraction routière. (Voy. C.J.U.E., 14 novembre 2013, *Baldž,* C-60/12, point 35). Cette interprétation est conforme à la jurisprudence de la Cour européenne des droits de l'homme qui applique le « test Engel » tel que déjà exposé ci-avant.
1591. Art. 44, § 3 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.,* 3 mai 2019.
1592. Pour l'APD voy. E. DEGRAVE, « Titre 11 – L'autorité de contrôle » in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie,* sous la coordination de K. ROSIER et C. DE TERWANGNE, Bruxelles, Larcier, 2018, p. 610.
1593. Les travaux préparatoires justifient cette interprétation restrictive en indiquant qu'à l'instar de toute loi spéciale dérogeant au régime général institué par le RGPD, elle doit être interprétée de manière stricte. De plus, le législateur rappelle que la directive 2016/680 succède à la décision-cadre 2008/977/JAI de sorte qu'il convient de veiller à ce que son champ d'application reste similaire. (*Doc. parl.*, Chambre, sess. ord., 2017-2018, n° 54-3126/001, p. 67)

public[1594] ; du Service d'enquête du Comité P dans le cadre de ses missions judiciaires[1595] ; de l'Inspection générale de la police fédérale et de la police locale ; de l'Administration générale des douanes et accises, dans le cadre de sa mission relative à la recherche, la constatation et la poursuite des infractions ; de l'Unité d'information des passagers[1596] ; la Cellule de traitement des informations financières ; du Service d'enquêtes du Comité R dans le cadre de ses missions judiciaires[1597]. La loi ne vise donc ni les services d'inspection sectoriel NIS ni celui de l'APD. En ce sens, les travaux préparatoires indiquent que les autres autorités administratives, même si elles ont des compétences de contrôle, d'inspection ou de poursuite de certaines infractions, ne sont pas considérées comme des autorités compétentes au sens du titre 2 de la loi du 30 juillet 2018[1598].

Même si cette approche pourrait sembler aller à l'encontre de l'esprit de la directive 2016/680 et limiter les garanties offertes aux personnes concernées, l'Autorité de la protection des données ne s'oppose pas à un tel régime soulignant que les activités de traitement (avec une finalité judiciaire) des instances et organes non compris dans le titre 2 et relevant du RGPD, peuvent relever de l'exception prévue par l'article 23 du RGPD[1599]. Cette disposition autorise les États membres à limiter, par mesures législatives, la portée des obligations et des droits des personnes concernées quant au traitement de leurs données[1600]. En conséquence, ce mélange de genre n'apparaît, à première vue, pas forcément préjudiciable pour la personne concernée, celle-ci disposant des droits et garanties conférés par le RGPD *a priori* plus étendus que ne le prévoit la directive 2016/680[1601].

Concernant la base de licité, le titre 2 de la loi du 30 juillet 2018 prévoit qu'un traitement est licite dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente dans le cadre des finalités visées par le titre 2 et s'il est fondé sur une obligation légale ou réglementaire. La base légale doit, au minimum, préciser les catégories de données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement[1602]. À juste titre, le titre 2, de manière similaire à la directive 2016/680, ne reprend donc pas les six bases de licéité du traitement du RGPD telles que l'intérêt légitime du responsable du traitement ou encore le consentement de la personne concernée[1603]. En effet, requérir le consentement par exemple, aurait peu de sens dans le domaine pénal ou de la justice où la personne est généralement tenue d'obtempérer au traitement de ses données et ne dispose donc pas d'une véritable liberté de choix[1604].

2. Les flux de données entre les autorités NIS, l'APD et les autorités policières

Dans le domaine de la cybercriminalité, la coopération entre autorités répressives, autorités publiques tels que le Centre pour la Cybersécurité Belgique (CCB)[1605] et acteurs pri-

1594. Plus précisément, il s'agit de l'ensemble des institutions dont la fonction est de faire appliquer la loi en tranchant des litiges tels les magistrats, les juridictions, les organes concourant à l'exercice du pouvoir de juger dans l'ordre judiciaires tels que les greffes les collèges des cours et tribunaux et le parquet. (Exposé des motifs, *Doc. parl.*, Chambre, sess. ord., 2017-2018, n° 54-3126/001, p. 60). En effet, l'instar des autorités répressives, les juridictions et les autorités judiciaires sont soumises au respect des dispositions relatives au titre 2 de la loi du 30 juillet 2018, notamment lorsqu'elles traitent des données à caractère personnel dans les décisions judiciaires ou les documents relatifs aux procédures pénales. Ceci ne saurait toutefois priver les Etats membres de préciser les opérations et les procédures de traitement dans leurs règles de procédures pénales' telle que le Code judiciaire ou le Code d'instruction criminelle. (Exposé des motifs, *Doc. parl.*, Chambre, sess. ord., 2017-2018, n° 54-3126/001, p. 67 et considérant 20 de la directive 2016/680).

1595. En vertu de l'article 16, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (*M.B.*, 26 juillet 1991), le Comité P est compétent pour « d'initiative ou sur réquisition du procureur du Roi, de l'auditeur militaire ou du juge d'instruction compétent, il effectue, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits mis à charge des membres des services de police (et de l'Organe de coordination pour l'analyse de la menace ».

1596. L'Unité d'information des passagers est un organe administratif qui reçoit, dans une première phase, des données à caractère personnel de compagnies aériennes dans le cadre de l'application du RGPD, mais couple, dans une deuxième phase, les données à caractère personnel à des données policières en vue de la prévention et la détection des infractions terroristes et des formes graves de criminalité ainsi que pour les enquêtes et les poursuites en la matière. (Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017).

1597. En vertu de l'article 40, alinéa 3, de la loi organique du 18 juillet 1991, le Comité R est compétent pour : « d'initiative ou sur réquisition du procureur du Roi, de l'auditeur militaire ou du juge d'instruction compétent, effectuer, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits à charge des membres des services de renseignement et de l'Organe de coordination pour l'analyse de la menace.

1598. *Doc. parl.*, Chambre, sess. ord., 2017-2018, n° 54-3126/001, p. 62.

1599. APD, « Avis 33/2018 relatif à l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », 11 avril 2018, p. 62.

1600. L'article 23, § 1er, du RGPD prévoit une possibilité de limiter sous certaines conditions la portée des droits garantis. La mesure considérée ne peut avoir pour effet de porter atteinte à l'essence des droits et libertés fondamentaux, elle doit être nécessaire et proportionnée dans une société démocratique pour garantir par exemple, la sécurité nationale, la sécurité publique, la prévention et la détection d'infractions pénales ou encore pour permettre l'exécution des demandes de droit civil. Si l'article 23, § 1er fait écho à l'article 52, § 1er de la Charte des droits fondamentaux, il complète néanmoins celui-ci par une série de critères devant spécifiquement figurer dans la disposition nationale. Celle-ci doit notamment prévoir des dispositions relatives « aux finalités du traitement ou des catégories de traitement », « aux catégories de données à caractère personnel » mais aussi « aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ».

1601. C. FORGET, La protection des données dans le secteur de la « police » et de la justice », in V. FRANSSEN et D. FLORE, *Société numérique et droit pénal. Belgique, France, Europe*, Bruxelles, Bruylant, 2019, pp. 865-900.

1602. Loi du 30 juillet 3018, art. 33.

1603. RGPD, art. 6.

1604. Directive 2016/680, consid. 35. Cette approche rejoint celle du RGPD selon laquelle le consentement ne peut être donné librement et constituer une base juridique valable pour le traitement de données à caractère personnel « lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ». (RGPD, consid. 43) En revanche, son consentement peut être requis en tant que garantie supplémentaire, en cas de traitement de données particulièrement sensibles par exemple pour pouvoir effectuer un test ADN dans le cadre d'une enquête comme le prévoit les articles 44*ter* et suivant du Code d'instruction criminelle.

1605. Voir notamment son rôle de CSIRT national – partie transposition de la directive NIS n°xx.

vés a pris une ampleur importante. À ce propos, la directive NIS rappelle qu'un incident « peut être le résultat d'activités criminelles, à propos desquelles la prévention, les enquêtes et les poursuites sont soutenues par la coordination et la coopération entre les opérateurs de services essentiels, les fournisseurs de services numériques, les autorités compétentes et les services répressifs. »[1606]. Partant, la directive invite les autorités compétentes et les autorités chargées de la protection des données à coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents[1607].

Cette coopération s'opère à différents stades. Tout d'abord, seuls les membres des autorités NIS sont tenus de dénoncer aux autorités répressives les infractions dont ils auraient connaissance, les inspecteurs de l'APD disposant à cet égard d'une certaine liberté. Ensuite, la loi permet expressément à l'APD de solliciter l'accès aux données traitées par les autorités NIS (Centre pour la Cybersécurité Belgique, le Centre de crise, les autorités sectorielles, les CSIRT sectoriels et les services d'inspections sectoriels) mais aussi à celles traitées par les autorités policières et judiciaires. Enfin, ces flux de données s'effectuent sans préjudice de la coopération volontaire qui, bien que non encadrée, n'échappe pas aux règles relatives à la protection des données.

a) L'obligation de dénonciation des autorités NIS

En raison de ses diverses compétences, le Centre pour la Cybersécurité Belgique reçoit de nombreux signalements des victimes d'infractions pénales tels que des infections par des *ransomwares* ou des attaques informatiques. Ces faits, s'ils sont portés à la connaissance du Centre pour la Cybersécurité Belgique, ne sont pas forcément également dénoncés auprès des services de police par l'entreprise concernée[1608]. Il n'en demeure pas moins qu'à l'instar de tout fonctionnaire, les membres du personnel du CCB, du Centre de crise, de l'autorité sectorielle et du service d'inspection sectoriel, lorsqu'ils ont la qualité d'officiers de police judiciaire ou de manière générique en tant que fonctionnaires, sont tenus d'avertir « sur le champ » le procureur du Roi des infractions pénales dont ils auraient connaissance dans l'exercice de leurs fonctions[1609]. On rappellera que cette obligation n'incombe pas aux inspecteurs de l'APD. En pratique, néanmoins, il paraîtrait assez naturel que les inspecteurs des autorités NIS puissent se montrer peu enthousiastes à l'idée de devoir dénoncer les infractions au magistrat du parquet. Ils prendraient en effet le risque de saper la confiance accordée par les opérateurs de services essentiels ou fournisseurs de services numériques leur dévoilant un incident de sécurité. En tout état de cause, la dénonciation d'une infraction s'effectue auprès des officiers de police judiciaire auxiliaires du procureur du Roi, chargés de renvoyer les informations au procureur du Roi, lequel examinera sans retard les procédures à mettre en œuvre[1610]. Ce magistrat est ensuite tenu de décider, sur

1606. Directive NIS, consid. 62.
1607. *Ibid.*, consid. 63.
1608. Circulaire 09/2017, p. 11
1609. Art. 29 CICr.
1610. Art. 53 et 54 CICr.

base des renseignements dont il dispose, s'il est raisonnable, utile, voire opportun d'exercer ou non l'action publique[1611].

Au niveau des règles relatives à la protection des données, un tel traitement est licite dans la mesure où il est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »[1612]. En ce cas, le RGPD suggère aux États membres d'encadrer la base légale en spécifiant notamment le type de données à caractère personnel devant faire l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les finalités, la durée de conservation ainsi que toutes autres mesures visant à garantir un traitement licite et loyal[1613].

b) Les demandes d'accès du service d'inspection de l'APD aux données détenues par d'autres autorités

La loi permet expressément à l'APD de solliciter l'accès aux données traitées par le CSIRT mais aussi à celles traitées par les autorités policières et judiciaires. L'article 68 de la loi sur l'APD indique en effet que les « services de l'État, y compris les parquets et les greffes des cours et de tribunaux, des provinces, des communes, des associations dont elles font partie, des institutions publiques qui en dépendent » sont tenus vis-à-vis de l'inspecteur général et des inspecteurs et à leur demande, de leur fournir tous renseignements qu'ils estiment utiles dans le cadre de leurs missions de contrôle[1614]. Les services de l'État peuvent également être tenus de produire des supports d'information et/ou des copies sous n'importe quelle forme[1615]. Cette disposition s'applique sans préjudice du respect de l'article 44/1 de la loi la loi du 5 août 1992 sur la fonction de police[1616] fixant les règles générales de la gestion des informations par les services de police[1617]. De surcroît, si les renseignements demandés font l'objet d'une enquête ou d'une information en cours, ils ne peuvent être communiqués que moyennant l'autorisation préalable du procureur du Roi ou du juge d'instruction[1618]. On rappellera à ce propos que l'information et l'instruction sont secrètes[1619] et passibles de sanctions pénales en cas de violation au même titre que les règles relatives au secret professionnel[1620]. De son côté, les membres de l'APD sont tenus par un devoir de confidentialité des faits, actes ou renseignements dont ils ont

1611. M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale*, Bruxelles, Editions Larcier, 2012, p. 265.
1612. RGPD, art. 6, c).
1613. *Ibid.*, consid. 45.
1614. Loi APD, art. 68, al. 1er.
1615. *Ibid.*, art. 68, al. 1er.
1616. *Ibid.*, art. 68, al. 2.
1617. A ce propos voy. M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, pp. 419-421.
1618. Loi APD, art. 68, al. 2.
1619. CICr, art. 28 *quinquies* et Art. 57.
1620. La violation du secret de l'instruction est punie d'un emprisonnement de huit jours à six mois et d'une amende de 100 à 500 euros. Voy. l'article 458 du Code pénal.

eu connaissance en raison de leurs fonctions[1621]. Ils peuvent conclurent des protocoles concernant le devoir de confidentialité avec des instances tierces afin de garantir l'échange des données nécessaires à l'exercice de leurs tâches et compétences[1622].

Concernant les autorités NIS, ces derniers peuvent également communiquer à l'APD des données fournies par les opérateurs de service essentiel et les fournisseurs de service numérique aux autorités belges ou étrangères, lorsque cet échange est nécessaire à des fins d'application de la loi[1623]. En ce cas, les informations échangées doivent se limiter à ce qui est pertinent et proportionné à l'objectif visé par cet échange conformément aux règles fixées par le RGPD[1624]. De surcroît, le responsable du traitement doit tenir compte du respect de « la confidentialité des informations concernées » mais aussi « de la sécurité et des intérêts commerciaux des opérateurs de services essentiels et des fournisseurs de service numérique »[1625].

c) La coopération volontaire

Examinons d'une part, le cadre légal applicable relatif à la coopération volontaire en tant que mesure d'enquête et d'autre part, les règles relatives à la protection des données.

i. La coopération en tant que mesure d'enquête

La coopération aussi efficace qu'elle soit, entraîne une atteinte aux droits et libertés des personnes concernées et en particulier, une ingérence dans le droit au respect de la vie privée[1626]. Pour être conforme aux règles fixées par la Convention européenne des droits de l'Homme, elle exigerait dès lors, une base légale pour pouvoir être mise en œuvre[1627]. En ce sens, partant du constat que l'aide volontaire d'acteurs privés ne peut constituer une

1621. Loi APD, art. 48, § 1er.
1622. *Ibid.*, art. 48, § 2.
1623. Art. 9, § 3, al. 1 de la loi NIS.
1624. Art. 9, § 3, al. 2 de la loi NIS.
1625. Art. 9, § 3, al. 2 de la loi NIS.
1626. Dans l'environnement numérique, les méthodes d'enquête entraînent essentiellement une atteinte dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel garantis par l'article 22 de la Constitution, l'Art. 8 de la Convention européenne des droits de l'homme et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Si le choix entre les différentes techniques d'enquête relève essentiellement du pouvoir discrétionnaire des Etats, ceux-ci ne disposent pas pour autant, d'une latitude illimitée. En vertu des articles 8, § 2 de la CEDH et 52, § 1 de la Charte, la procédure applicable doit s'inscrire dans le respect des critères de légalité, de nécessité et de proportionnalité en vue de prémunir la personne concernée contre les risques d'ingérences illicites ou arbitraires des pouvoirs publics.
1627. Le critère de légalité exige une réglementation « claire, prévisible et accessible » assurant une protection contre les risques d'abus et d'arbitraire et permettant au justiciable, si besoin en s'entourant de conseils éclairés, de régler sa conduite. (Cour EDH, *Sanoma Uitgevers B.V. c. Pays-Bas*, 14 septembre 2010, n° 38224/03, § 81).

base solide pour la coopération[1628], le Conseil de l'Europe constate que la coopération public/privé ne saurait se soustraire à l'État de droit. Déjà auparavant en 2008, dans le cadre des lignes directrices pour la coopération entre organes de répression et « fournisseurs de services Internet » au sens large[1629], le Conseil de l'Europe encourageait « les forces de l'ordre à élaborer des procédures écrites, incluant les mesures appropriées d'application, pour l'émission et le traitement des requêtes pénales, et pour s'assurer que ces requêtes soient prises en charge dans le respect des procédures agréées. »[1630]. Les requêtes devraient par exemple, contenir au minimum : un numéro d'enregistrement, la référence aux textes juridiques de base, les données spécifiques sollicitées et les informations permettant de vérifier la source de la requête[1631]. Dans la même lignée, une proposition de directive de 2011, encadrait la possibilité pour les autorités répressives de solliciter des données auprès d'acteurs tiers. Tout d'abord, la demande devait démontrer l'existence d'un motif raisonnable de croire que le traitement des données à caractère personnel contribuerait substantiellement à la prévention, à la recherche, au dépistage ou à la répression d'infractions pénales ou à l'exécution des sanctions pénales[1632]. Ensuite, les demandes d'accès devaient être formulées par écrit et indiquer le fondement juridique de la demande[1633]. Enfin, des garanties appropriées devaient être mises en place pour assurer la protection des droits et libertés fondamentales en matière de traitement des données à caractère personnel[1634] dont subordonner l'accès aux données à des conditions supplémentaires telles qu'une autorisation judiciaire[1635]. Cette proposition n'a toutefois pas été retenue[1636].

1628. CyberCrime@EAPIII, General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, septembre 2016. Le rapport est disponible sur : https ://rm.coe.int/16806a5b8f.
1629. Ce terme est entendu de manière large et vise, conformément à l'article 1 de la Convention de Budapest : « Tout entité publique ou privée offrant aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique » mais aussi « tout autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs. ».
1630. Conseil de l'Europe, « *Lignes directrices pour la coopération entre organes de* répression et fournisseurs *de* services Internet *contre* la cybercriminalité », 2 avril 2008, Point 18, disponible sur [https ://rm.coe.int/16802fa3a7]
1631. Conseil de l'Europe, « *Lignes directrices pour la coopération entre organes de* répression et fournisseurs *de* services Internet *contre* la cybercriminalité », 2 avril 2008, Point 18, disponible sur [https ://rm.coe.int/16802fa3a7]
1632. Proposal for a directive of the european parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, version 34, 29 novembre 2011, art. 4, § 2, A).
1633. *Ibid.*, art. 4, § 2, B).
1634. *Ibid.*, art. 4, § 2, C).
1635. *Ibid.*
1636. A ce propos voy. C. JASSERAND, « Law enforcement access to personal data originally collected by private parties : Missing data subjects' safeguards in Directive 2016/680 ? », *Computer Law & Security Review*, n°34(1), pp. 154-165.

Malgré les obligations légales de coopération encadrée par le Code d'instruction criminelle dans les conditions examinées *supra*, la loi n'encadre pas la coopération volontaire. On peut néanmoins noter que le considérant 31 du RGPD indique que « les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement ». En effet indépendamment de l'existence d'un cadre légal – ou d'une absence de cadre légal – relatif à la coopération volontaire, le responsable du traitement lorsqu'il communique des données à caractère personnel à une autorité judiciaire ou administrative, est tenu au respect des règles relatives à la protection des données et en particulier, la base de licéité du traitement mais aussi les droits des personnes concernées.

ii. La base de licéité du traitement

Dans le cadre d'une coopération volontaire entre un acteur tiers et une autorité policière, le consentement des personnes concernées n'est pas nécessaire pour établir la base de licéité du traitement, « l'intérêt légitime » du responsable du traitement ou d'un tiers autorisé à traiter les données étant suffisant[1637]. L'appréciation de « l'intérêt légitime » repose sur le principe de responsabilité. Il appartient au responsable du traitement d'effectuer « une analyse minutieuse et effective, fondée sur les circonstances factuelles particulières plutôt que sur une réflexion abstraite »[1638]. Tout d'abord, le responsable du traitement doit déterminer l'intérêt poursuivi et veiller à le distinguer de la finalité poursuive même si elle peut lui être étroitement liée[1639]. La finalité est la raison pour laquelle les données sont traitées, le but, tandis que l'intérêt est compris de manière large et vise le bénéfice qu'il tire ou que la société au sens large pourrait tirer du traitement[1640]. Cet intérêt doit être « légitime », autrement dit, être « acceptable au regard du droit » par exemple, s'il souhaite dénoncer des dysfonctionnements ou encore des situations frauduleuses.

Une fois cet intérêt légitime défini, le responsable du traitement est tenu d'effectuer une mise en balance des intérêts en présence afin de s'assurer que pour atteindre l'objectif visé[1641], il n'existe pas d'autres moyens moins intrusifs pour la personne concernée. En

1637. En ce sens, le considérant 50 du RGPD indique que « le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante ».
1638. Groupe 29, « Avis 06/2014 », p. 48.
1639. *Ibid.*, p. 26.
1640. *Ibid.*
1641. *Ibid.*, p. 32.

effet, il faut que « ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée »[1642]. À cet égard, le responsable du traitement doit tenir compte des « attentes raisonnables » de cette dernière, autrement dit, il doit examiner « si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée »[1643]. Dès lors, le RGPD précise que « les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur. »[1644]. Un intérêt légitime impérieux, en cas de criminalité grave par exemple, peut toutefois justifier, dans certains cas une ingérence importante dans la vie privée[1645].

iii. Les droits des personnes concernées : information et transparence

Comme précisé ci-devant, en définissant l'intérêt légitime poursuivi, le responsable du traitement doit tenir compte des droits des personnes concernées et chercher à réduire indubitablement et sensiblement les incidences du traitement sur ses droits[1646]. À titre illustratif, celles-ci peuvent consister en une limitation stricte du volume de données collectées, la suppression immédiate des données après utilisation, des mesures techniques et organisationnelles visant à garantir une séparation fonctionnelle, l'utilisation appropriée de techniques d'anonymisation, l'agrégation des données, et des technologies renforçant la protection de la vie privée, mais aussi plus de transparence, de responsabilité et la possibilité de s'opposer au traitement[1647].

Ces différentes garanties peuvent être mise en œuvre sans préjudice des obligations incombant au responsable du traitement de respecter les droits des personnes concernées et en particulier, le droit à l'information. Conformément au principe de loyauté[1648] et de

1642. RGPD, art. 6, f).
1643. *Ibid.*, consid. 47.
1644. *Ibid.*, consid. 47.
1645. Ce raisonnement a été étayé à plusieurs reprises par le Groupe 29 notamment dans l'avis relatif aux « lanceurs d'alerte » (Groupe 29, « Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes in ternes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière », 1er février 2006).
1646. Groupe 29, « Avis 06/2014 », p. 34.
1647. *Ibid.*, p. 47.
1648. L'exigence de loyauté implique que le responsable du traitement ne dissimule pas certaines informations et n'agisse pas par tromperie (C. DE TERWANGNE, « Principes de base de la protection des données » *in* Le règlement général sur la protection des données : Analyse approfondie, (sous la coordination de K. ROSIER et C. DE TERWANGNE), Bruxelles, Larcier, 2018, p. 90).

transparence[1649], une personne doit être informée de l'existence d'une opération de traitement et de ses finalités[1650] mais aussi, des risques, des règles, des garanties et des droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement[1651]. Dès lors, lorsque le responsable du traitement a l'intention de traiter les données à caractère personnel à d'autres fins que celles pour lesquelles les données ont été initialement collectées, celui-ci devrait, avant de procéder à ce traitement ultérieur, fournir à la personne concernée des informations au sujet de cette autre finalité[1652].

F. Conclusion

Face aux « menaces » informatiques, le législateur européen, puis national, a bétonné en profondeur notre arsenal législatif relatif à la protection des données. En ce sens, la lutte contre la cybercriminalité est qualifiée par le Contrôleur européen de la protection des données de « pierre angulaire du renforcement de la sécurité et de la sûreté dans l'espace numérique et de l'instauration de la confiance nécessaire »[1653]. Ce renforcement implique d'offrir aux différentes autorités, en l'occurrence, l'APD et le CSIRT, des compétences suffisantes pour leur permettre d'enquêter et de s'assurer du respect des lois soumises à leur contrôle. Dans ce cadre, le législateur a décidé d'offrir la qualité d'officier de police judiciaire aux inspecteurs du CSIRT, et non aux membres du service d'inspection l'APD. Ces derniers conservent dès lors une certaine indépendance : ils ne sont pas soumis aux directives du procureur du Roi et ne sont pas tenus par une obligation de dénonciation auprès des autorités répressives. En plus, la loi sur l'APD prévoit une obligation de collaboration dans le chef des personnes qui font l'objet d'un contrôle, ce que ne prévoit pas la loi NIS. En revanche, les inspecteurs de l'APD ne peuvent exercer les compétences fixées dans le Code d'instruction criminelle, contrairement aux enquêteurs du CSIRT. On précisera néanmoins que certaines mesures plus intrusives pour les droits et libertés des personnes concernées, telles que l'obligation de collaboration ou le repérage des communications en cas de flagrant délit, ne peuvent être déléguées qu'aux officiers de police judiciaire « auxiliaire du procureur du Roi », qualité que la loi NIS n'accorde pas aux inspecteurs du CSIRT.

1649. Ce principe doit permettre à la personne concernée d'être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées. (Groupe 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 », adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018, p. 8).
1650. RGPD, consid. 60 et art. 13, §§ 2-1.
1651. Il s'agit des informations telles que libellées à l'article.
1652. RGPD, art. 13, § 3.
1653. CE, Résumé de l'avis du Contrôleur européen de la protection des données relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité, [2012] JO, C 336 à la p 7.

Quoi qu'il en soit, la coopération entre ces différents services et les autorités répressives est patente puisque tant les inspecteurs de l'APD que ceux du CSIRT peuvent requérir l'assistance des services de la police fédérale ou locale pour mener à bien leurs missions. En outre, l'APD peut imposer aux services de l'État, y compris les parquets, de fournir certaines données, sous réserve du secret de l'information et de l'instruction. Ces différentes formes de coopération s'exercent sans préjudice de la coopération volontaire qui, bien qu'en principe admissible au niveau des règles relatives à la protection des données, ne souffrirait pas de bénéficier d'un encadrement légal adéquat, le Conseil de l'Europe rappelant que l'aide volontaire d'acteurs privés ne pourrait constituer une base solide pour la coopération entre tiers et autorités répressives[1654].

1654. CyberCrime@EAPIII, General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, septembre 2016. Le rapport est disponible à l'adresse suivante : https ://rm.coe.int/16806a5b8f.